Unclassified
April 2006
No. 88

Canadian Security Intelligence Service

Commentary

Between Probity and Proficiency: Challenge and Change within the Australian Intelligence Community

Michael Wesley

The publication of *Commentary* is intended to provide a platform for public discourse on issues related to national security.

1. Introduction

The Australian Intelligence Community (AIC) appears to undergo significant reform at quarter-century intervals. Australia's core collection agencies, the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Australian Security Intelligence Organisation (ASIO) were developed at the end of the Second World War. Then in the late 1970s, the Commonwealth created a new intelligence analysis and co-ordination agency in the Office of National Assessments (ONA), separate from the Defence Intelligence Organisation (DIO) and formalized the principles of functional differentiation and oversight. These arrangements operated largely undisturbed by organizational reforms to the rest of the bureaucracy until 2004, when as a result of new pressures, controversies, inquiries and reports, a new set of reforms were enacted. Both the everyday operation of the AIC and each period of major reforms to Australia's intelligence architecture have been guided by three powerful organizing principles: functional specialization in intelligence collection; the separation of intelligence collection and assessment; and the separation of domestic and foreign intelligence collection and assessment. Recently, at a time when some of Australia's closest allies have considered major structural changes to their intelligence communities, Canberra has engaged in more modest reform, which has underlined and strengthened, rather than challenged, these basic organizing principles.

The most recent reforms to the AIC are a response to two linked sets of stimuli. One is the quickening pace of globalization, which is changing the nature, volume and urgency of the demands on all states' intelligence agencies. If the 1990s were an era that had celebrated the benefits of globalization, the key preoccupation of the first decade of the twenty-first century would be to come to terms with globalization's dark sides. The other stimulus was a series of high-profile controversies relating to the AIC. In 1999 the defence intelligence agencies became embroiled in allegations that intelligence on the activities of Indonesian-backed militias in East Timor had been ignored and withheld from field units of the Australian Defence Force and from Australia's closest allies. The scandal deepened with the suicide of an Australian Defence Intelligence Liaison Officer in Washington, and the charges were reiterated in 2004 in the midst of later intelligence controversies. In 2001, ONA was criticized for fabricating intelligence to support the government's case over the actions of asylum seekers, and DSD was accused of illegally eavesdropping on Australian citizens acting on behalf of the asylum-seekers. The October 2002 Bali bombing, which caused the deaths of 88 Australians, saw questions raised about whether Australian intelligence had taken sufficiently seriously the threat of violent Islamic groups in Southeast Asia. Then in 2003, the AIC came under sustained scrutiny for its role in providing justifications for Australia's participation in the March 2003 invasion of Iraq.

The result was a series of commissioned and parliamentary inquiries into the operations and adequacy of the AIC. Particularly in the context of a bitter partisan debate over the invasion of Iraq in the lead-up to the 2004 federal election, these inquiries attracted unprecedented attention to the intelligence agencies. The culmination of the review process came with the inquiry conducted in 2004 by former ONA Director-General Philip FLOOD, which resulted in a package of 23 reform

proposals being presented to the government, all but one of which were implemented.[1] My aim in this article is to examine the Australian government's recent reforms to the AIC in light of new pressures facing intelligence agencies and allegations of "intelligence failures" against the AIC.

1. Pressures on Intelligence

Australia's intelligence agencies, like those of its closest allies, face a brace of challenges arising from the processes of globalization. Over more than a decade, globalization has transformed the nature of threats faced by modern societies, the capacities of both intelligence agencies and their targets, and the political and diplomatic context within which intelligence agencies operate. The challenges posed to intelligence agencies by transnational threats are complex, and most intelligence communities are still evolving in response. While terrorism is a top national security priority in most Western countries, the proportion of intelligence resources devoted to other transnational challenges is very small. Currently in Australia as in many other countries, the challenge is to ensure that the intelligence effort against terrorism does not too drastically pull resources away from traditional targets and tasks. This may change if other transnational issues have as dramatic an effect on the public psyche as terrorism has recently.

Transnational challenges

The demise of Cold War confrontation and the forces of globalization have raised transnational threats to the forefront of national security, and thus brought them to the centre of the work of intelligence agencies. Transnational issues can be defined as those that arise from within one or more societies (rather than from within the decision structure and resources of the state) and are transmitted or replicated across national borders to threaten the security or values of society — and ultimately the security or viability of the state. They include terrorism, sub-state proliferation of WMD and missile technology, organized crime, drug production and distribution, serious disease epidemics, irregular people movements, illegal resource exploitation, and disruptive doctrinal movements.[2] Most transnational issues are the work of decentralized, transactional networks of non-state actors distributed across several societies, interacting amidst the vast quantity of transactions occurring daily in a globalized world. Linkages among transnational actors are increasingly made on the basis of either shared general goals or common interests in a particular transaction, rather than being based on ethnic- or family-based loyalties or formal command structures. As a result, the most dangerous transnational threats we face are beginning to exhibit what biologists term 'emergent behaviour', where the dynamic interactions of agents reacting to local situations give rise to collective behaviours that are more flexible and complex than a centralized, hierarchic organization could manage. Globalized communications enable far-flung groups to observe and adapt the most effective techniques they see used elsewhere. Often the most dangerous transnational flows are not

---

[1] Commonwealth of Australia, *Report of the Inquiry into Australian Intelligence Agencies, July 2004*, Canberra: Goanna Print, 2004

[2] Michael WESLEY, "Analysing Transnational Intelligence", in Carole DUMAINE and L. Sergio GERMANI (eds) *New Frontiers of Intelligence Analysis*, Collected Conference Papers, Sherman Kent School for Intelligence Analysis, 2004

people or goods but information – be it the doctrine of world jihad, gas centrifuge designs, synthetic amphetamine recipes, or how to make shape-charges.

Transnational threats challenge long-established understandings of security and international relations. States such as Australia have come to realize that the major contemporary threats they face are not those posed by other states to their military-industrial power or their institutions of state. Rather, transnational threats, from terrorism to crime and drugs and disease pandemics, endanger the understandings and practices of civic association that are so basic to the functioning of modern societies. Not only does globalization transmit transnational threats across borders more rapidly and extensively than ever before, it has magnified what Emile DURKHEIM described as the greater "organicism" of modern societies — meaning the advancing interdependence and greater functional specialization of actors and institutions.[3] The growing specialization and patterns of interaction in modern societies, their growing dependence on information technologies and "just-in-time" inventory and production systems, and their increasing impatience with redundancy have led to huge increases in their vulnerability to catastrophic disruption.[4] As a result, transnational threats are blurring the distinction between domestic and international intelligence collection, as well as that between the public/state sphere and the private/societal sphere of security.[5] There has been a major transformation in the role of foreign intelligence organizations. Rather than concentrating only on discovering the capabilities and intentions of other states, foreign collection and analysis agencies have been drawn increasingly into the realm of their domestic security counterparts, monitoring the actions, intentions and influences of individuals and groups that could eventually threaten the lives and livelihoods of Australians. And as transnational issues widen the range of security threats to states, more government departments are being drawn into the business of national security and are becoming the consumers and collectors of intelligence. The vulnerability of societies and their infrastructure to terrorist attack has brought immigration, health and transport departments into security structures and made the information available through their bureaucratic networks vital to intelligence early warning systems.

Transnational threats, by their nature and volume, pose major difficulties for intelligence organizations accustomed to focusing on the activities of states and their agents. The standard methods of Western intelligence agencies were originally developed to collect and interpret intelligence on a few secretive but rigidly hierarchic and centralized states – usually on policies, dispositions and capabilities that were developing in a single, coherent direction over decades. The major challenge facing intelligence collection and assessment on decentralized, transactional networks arises from their absence of a clear hierarchy of command and control. Consequently, the real challenge for collection and analysis is assessing the value of the intelligence gained. Reporting

---

[3] Emile DURKHEIM, *The Divisions of Labour in Society*, (New York: Free Press, 1984).

[4] MICHAEL WESLEY, "Towards a Realist Ethics of Intervention", *Ethics and International Affairs*. This problem has been somewhat more polemically discussed by Ulrich BECK in his Risk Society, Towards a New Modernity, trans. Mark RITTER, (London: Sage Publications, 1992).

[5] Gregory F. TREVERTON, 'Reshaping Intelligence to Share with "Ourselves"', *CSIS Commentary*, No. 82, Summer 2003, p. 5.

on the intentions of one or several actors in a transnational network gives intelligence agencies a highly uncertain picture of the intentions and capabilities of the network as a whole. And as decentralized actors constantly adapt their behaviour to deal with local requirements, it is difficult to build a dependable picture of the network incrementally. There are challenges here for both collection and analysis agencies.

Collectors of intelligence on transnational threats increasingly have to do their own on-the-spot analysis in order to validate information and prioritize collection targets against a rapidly evolving organization. Advances in information technology, and greater publicity about the methods of collection agencies have complicated the process of intelligence collection. Individuals and organizations are now able to acquire cheap and highly effective encryption technologies and use a range of Internet innovations to disguise their communications. Even as SIGINT organizations race to keep one step ahead of these technologies and tricks, transnational actors have resorted to a range of "low-tech" strategies, placing greater pressure, in turn, on HUMINT collectors to find clues to their activities. And as states increasingly deploy to anticipate and block transnational threats, collection agencies are devoting more and more of their resources to supporting overseas operations of defence and police forces, as well as their own disruption operations, as opposed to collecting for analysis. At the same time, the state's deployed defence and police forces are generating large volumes of valuable intelligence that need to be gathered and evaluated by the collection and analysis organizations.

Against transnational threats, intelligence analysis agencies face an asymmetric contest. For terrorists and criminals in decentralized networks, every problem is local and dealt with locally, whereas the intelligence effort is required to try to grasp the entire problem. The art becomes that of abstracting and anticipating behavioural patterns and possibilities, rather than seeking definite answers. In the words of one commentator, against transnational threats, "many questions cannot be resolved as a matter of logic because they depend on events yet to happen, such as human intentions that will unfold or factors that will converge by chance."[6] Transnational intelligence analysis is required not only to assess warnings of emerging threats and reports on strategic trends in transnational threats, it is also being drawn into tactical analysis geared towards enforcement operations, greatly expanding the demands on the limited resources of analytical agencies.

Political and diplomatic contexts

In creating a public climate of apprehension and a new set of imperatives for government action, transnational threats have also changed the political context in which intelligence agencies operate. Particularly since the September 11 attacks, intelligence agencies have evolved in the public mind from arcane "spy-versus-spy" operations toward a more accepted role in protecting society, more akin to the defence forces and law enforcement agencies. Intense media reporting of intelligence inquiries both in Australia and overseas and a profusion of polemics and exposés, often by disgruntled former intelligence staff, have raised public awareness and knowledge of the AIC and

---

[6] Lee S. STRICKLAND, "The Information Shortcomings of 9/11", *Information Management Journal*, 38:6, November/December 2004, p. 43

its practices. One frustration of many intelligence professionals is that intelligence agencies are unable to answer many of their critics, which leaves the field open to distortions and misunderstandings. As the intelligence agencies have received greater funding and powers in the aftermath of September 11, it is inevitable that public expectations of their omniscience will have been reinforced. Repeated references to "intelligence failures" and a public culture of looking for someone to blame for terrorist attacks have worked against government attempts to lower public expectations. There is still a very low level of public understanding of the capacities and limitations of intelligence agencies, an issue that calls for better public information. While the majority of the Australian public appears supportive of the role of intelligence in combating terrorism, some critics have worried that their role represents the vanguard of a national security state. The intense debate over ASIO's enhanced powers of detention and questioning has heightened public awareness of individuals' legal rights, and prominent role of the AIC leading up to and after the war in Iraq has decreased the willingness of some groups and individuals to co-operate with the intelligence community.

The impact of terrorism on democratic politics has greatly complicated the political context within which intelligence agencies work. In Australia, the psychological impact of the September 11 attacks coincided with a sudden rise in the number of sea-borne asylum seekers heading for the island continent to create a pervasive atmosphere of threat, in which stewardship of national security joined the capacity to manage the national economy as the two key tasks of government in the minds of the vast majority of the electorate. Governments wanting to burnish their "national security credentials" in the face of oppositions equally keen to tarnish those credentials have elevated public safety to the highest possible policy priority. In a climate of public fear of terrorism, nothing can be left undone in the interests of public safety. Intelligence and law enforcement agencies, identified as the best way of protecting society from transnational threats, have been granted greater resources and powers. Amid the partisan competition over national security credentials, media and parliamentary scrutiny has grown. Opposition parties are increasingly keen to use parliamentary committees – and especially the annual Senate Estimates Committee hearings – to probe intelligence chiefs over issues thought to erode the electorate's trust in the government's management of national security. Intelligence agencies and their political masters realize that any event deemed an "intelligence failure" could and has resulted in their practices, thoroughness and judgments being subjected to the detailed scrutiny of the media and parliament, both acting with the wisdom of hindsight.

In this atmosphere, overlooked, misjudged or unactioned intelligence information can be political dynamite. Intelligence agencies must ensure that all credible threat intelligence is passed on to government, and governments are expected to pass threat warnings on to the public in the form of travel advisories. Placed squarely in the front line of protecting society from transnational threats, intelligence agencies have become worried they will miss the significance of a piece of intelligence warning of an impending attack. Facing the choice of not reporting a piece of intelligence and risking it might be genuine, however spurious it may look, the natural temptation is to report it. If not resisted, the onus of evaluating and reacting to threat intelligence would be pushed to higher and higher levels of government, challenging the very reason for being of intelligence analysis agencies. The political imperatives of transnational threats also magnify the time pressures on agencies confronted by an avalanche of intelligence information of highly variable quality. Intelligence

organizations are required to present their customers with high-quality intelligence and hard baseline judgments and predictions in a timely manner, while the intelligence is still 'fresh'. This leads inevitably to evaluation and analysis having to make judgments on the basis of the information at hand, without being able to await confirmation or a fuller picture. It also means that collectors and analysts are rarely in a position in which they can spend time trying to verify the information they have received. The need for real-time analysis has only been increased by the flow of raw intelligence to ministerial offices and policy departments — a development that is likely to be permanent given ministerial appetites for intelligence and the collection agencies' interest in expanding their customer base — as ministerial offices and policy departments increasingly demand immediate analysis of the credibility of incoming intelligence. To add to these pressures, Australian government ministers and their senior advisors, many of whom have occupied national security portfolios for a decade and regularly meet to discuss intelligence-informed issues in the powerful National Security Committee of Cabinet (NSCC), have become much more experienced and discerning consumers of intelligence.

The rise of transnational threats has also seen Australia's intelligence agencies drawn into the world of diplomacy. While the underlying adversarial logic of intelligence still persists among states, the very nature of transnational threats mandates greater co-operation among countries. Developed states' concerns about "failing states" – weak parts of the fabric of international order in which terrorists, criminals and proliferators lodge and transit – have coincided with developing states' concerns to reassure the outside world, and in particular investors and tourists, of their commitment to good governance. Transnational threats have increased the intimacy of Australia's UKUSA intelligence-sharing relationship with America, Britain and Canada, even while eroding its geographic specializations. In the words of one manager in a collection agency, "simply watching your 'patch' won't cut it any more with customers or partners." Australia's intelligence and law enforcement agencies have been at the forefront of regional co-operation against transnational threats: collaborating with counterpart agencies in field investigations, training their counterparts in regional countries, and participating in an ever-expanding network of exchange of intelligence material and judgments on transnational threats outside of traditional alliance structures. In addition to the time demands on already stretched organizations, "intelligence diplomacy" and the resulting sharing of intelligence and tradecraft give rise to fears about the protection of sources and methods and the effect that co-operation will have on these states' future counter-intelligence capabilities. Expanded intelligence liaison has also delivered a greater amount of intelligence material of uncertain reliability for intelligence analysis organisations to cope with.

2. Intelligence Failures

Despite the controversy surrounding Australia's intelligence agencies since 1999, two issues had become the focus of inquiry and debate by 2004: whether the AIC had underestimated and overlooked the threat of radical Islam in Southeast Asia prior to the October 2002 Bali bombings; and whether the AIC had oversold the possibility that Iraq possessed weapons of mass destruction (WMD) before the March 2003 invasion. Australia's controversies and inquiries closely mirrored those in the United States and United Kingdom over terrorist attacks (September 11 and Iraq for the US, the Bali bombing and Iraq for the UK), and many of the accusations, arguments and judgements

made in Australia were influenced by those in America and Britain. In Australia, as in the United States and the United Kingdom, three basic categories of intelligence failure were highlighted. First was a range of issues relating to the collection and distribution of intelligence: overloading and failing to properly evaluate sources; allowing assumptions to guide collection targeting; failing to pass information between agencies. Second were failures of imagination: either allowing preconceptions to blinker creative thinking or allowing "satisficing"[7] deductions to crowd out the consideration of alternative explanations. Third were issues relating to "politicization": whether intelligence agencies had allowed their judgements to be influenced either overtly or subliminally by the preferences of governments seeking to make compelling cases to go to war. The first two categories are familiar shortcomings of intelligence: problems of source evaluation, information-sharing and cognitive rigidity have been recognized for a long time, and have spawned a considerable literature. The third category, raising issues of the intelligence-policy interface and the public use of intelligence, is much newer. The recurring nature of "old" intelligence failures poses particular challenges to intelligence reform; while "new" challenges raise a range of different considerations.

Familiar failures

The failure of the Iraq Survey Group (ISG) to find evidence of the WMD that the American, British and Australian governments had alleged Iraq possessed prior to their invasion was seized on by opponents of the war to support charges that the coalition governments had misled their electorates over the reasons for going to war. As the governments' prewar statements on Iraq's WMD stocks and activities were picked over, it was inevitable that the intelligence agencies, on whose material and judgements these claims had been based, would become drawn into the controversy. As the debate continued, three particular pieces of intelligence that had contributed to judgements that Iraq was developing a "breakout" WMD capability came under the spotlight. They were reports that Iraq had attempted to negotiate the sale of uranium from Niger; reports that Iraq had imported large quantities of high-grade aluminium tubes and magnets that could be used to construct gas centrifuges for enriching uranium; and that the Saddam HUSSEIN regime had developed several mobile laboratories for manufacturing biological weapons (BW). Each of these pieces of intelligence were cited by the Australian, British and American governments in speeches arguing the case for war, and each of them had been publicly discredited shortly after the war. The Italian newspaper *La Repubblica* published photos of obviously forged documents on which at least some of the reports of Iraq's attempts to buy uranium from Niger had been based, and former American diplomat Joseph WILSON made public the negative findings of his official mission to Niger to check the claims.[8] Scientific experts testified to the International Atomic Energy Agency (IAEA) prior to the war that the aluminium tubes, unless significantly modified, were unsuitable for use in a uranium enrichment centrifuge. And the vehicles thought to have been mobile BW laboratories were found by the ISG

---

[7] A course of action that is "good enough" - that satisfies. ALLISON, Graham T. "Essence of Decision-making. Exploring the Cuban Missile Crisis", 1977.

[8] The UKSIS has continued to assert the validity of the Iraq-Niger uranium claims, based on a HUMINT source it has refused to discuss further.

to have been intended for other purposes; in late 2005, officials in Germany's Federal Intelligence Service revealed that the CIA had been overly credulous in accepting claims of an unreliable Iraqi defector codenamed "Curveball" about the mobile BW laboratories.[9]

The post-war intelligence inquiries in the United States, the United Kingdom and Australia all criticized their respective collection and analysis agencies for failing to properly scrutinize the claims of HUMINT sources. The Australian inquiry, held by the Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD), cited the arguments of a witness to the UK's Hutton inquiry, that human intelligence collection agencies have an incentive to overemphasise the reliability of their sources in the interests of demonstrating their relevance and usefulness to intelligence consumers. The Butler inquiry in Britain found that intelligence agencies' increasing sense of urgency to clarify Iraq's WMD holdings and capacities had led HUMINT collectors to put more pressure on sources: either relying more heavily on untried sources, accepting reporting chains whose length would have been unacceptable in other circumstances, or pressing sources to report on issues outside of their areas of expertise.[10] In Australia, ASIS escaped much of the criticism endured by its American and British counterparts due to the fact that perhaps 97 per cent of the raw intelligence informing Australia's intelligence judgements came from allied sources. This, however, raised specific issues for Australian intelligence. Shared human intelligence must ultimately be taken on trust, with the assumption that allied HUMINT collectors would only pass on intelligence they had deemed to be credible. Source descriptors on pieces of HUMINT must necessarily be general in the interests of source protection; and given the massive increase in the amount of reporting collection agencies have been required to do, these descriptors had tended to become formulaic, choices from a "pull-down" menu on a computer program. Despite these caveats, however, Australia's analysis agencies were accused of being insufficiently critical in assessing their claims. The Office of National Assessments in particular was accused, like its counterparts in the United States and United Kingdom, of drawing too strong a set of judgements from the available intelligence. As the PJCAAD sternly admonished in its report, "Decisions to go to war, with the potential to cost many lives, must only be taken on the basis of the soundest information, information that Australian agencies can reasonably rely upon."[11]

As the shock of the Bali bombings percolated through Australian society, questions began to be asked whether this terrorist attack had been preceded by the same type of intelligence failures that were emerging concerning the September 11 attacks. Attention soon focused on the Web site of the Department of Foreign Affairs and Trade (DFAT), which warned at the time of the attacks that the threat of violence in Indonesia was "high", but also stated that "tourist services in other parts of the country, including Bali, [were] operating normally." It also emerged that the United States had issued

---

[9] See Bob DROGIN and John GOETZ, "U.S. Whiffs on 'Curveball': Close Up", *The Los Angeles Times*, 27 November 2005

[10] The Rt. Hon. The Lord BUTLER of Brockwell KG GCB CVO, *Review of Intelligence on Weapons of Mass Destruction*, Report of a Committee of Privy Counsellors, House of Commons, London: The Stationery Office, 2004, p. 108

[11] Commonwealth of Australia, *Intelligence on Iraq's Weapons of Mass Destruction*, Report of the Parliamentary Joint Committee on ASIO, ASIS and DSD, Canberra:CanPrint Communications, December 2003, p. 74 (hereafter referred to as "PJCAAD Report")

a travel warning concerning Bali in late September 2002, and that the United States Ambassador to Australia had delivered a warning concerning impending attacks in Bali to the Australian government the day before the attacks occurred.[12] In the United States, as the September 11 post-mortems continued, evidence was emerging that the American intelligence community had warnings of impending attacks, but that different agencies had either failed to pass information to each other, or had failed to act on information that was passed on; the 9/11 Commission later spoke of a "void" between coverage of foreign and domestic threats.[13] Was Bali similarly a "preventable" tragedy, allowed to occur because Australian agencies had failed to communicate?

A parliamentary inquiry found that no specific intelligence could have warned of an impending attack in Bali in October 2002. Instead, controversy focused on another site: that intelligence assessments about the danger posed to foreigners in Indonesia by radical Islamic groups was not "adequately reflected" in the DFAT Travel Advice.[14] In their testimony to the Inquiry, DFAT and ASIO had admitted there was no joint consultation on the preparation or wording of Travel Advice, and that their roles had been "too compartmentalised". But beyond this isolated problem, there was a degree of confidence in the AIC that the same scale of communication and responsibility failure would not occur in Australia, where ASIO had long been understood to be the lead agency on terrorist threats. The ASIO Act makes clear that its responsibility is security intelligence – whether domestic or foreign – not simply domestic intelligence. It had always been the case that ASIO, in addition to its own domestic intelligence collection, gains full access to all relevant foreign intelligence collected by the AIC.

But this does not mean there is complacency in the AIC about potential communication problems. The proliferation of parts of government involved in intelligence in the age of transnational threats necessitates good communication with agencies unfamiliar with the practices and understandings of the AIC. Here the wider intelligence community faces issues of maintaining security, information technology connectivity, and most importantly, differences in informational culture. Organizations with different informational cultures have different understandings of what is important intelligence and what is background, what can and should be shared and what shouldn't. The biggest potential challenge here lies in establishing effective and seamless communications with the Australian Federal Police (AFP), whose external operations are the source of a wealth of valuable intelligence on transnational threats. Intelligence work is essentially forward-looking, seeking to predict and forestall emerging threats to state and society; police work usually involves collecting evidence on a case-by-case basis after a crime has been committed. As one witness told the 9/11 Commission, foreign intelligence organizations tend to play "zone defence", watching for patterns and developments in geographic areas of responsibility, whereas law enforcement agencies play "man

---

[12] New York Times, 20 October 2002

[13] Philip ZELIKOW et al., *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized Edition, New York: WW Norton and Company, 2004, p. 263

[14] Commonwealth of Australia, *Bali 2002: Security Threats to Australians in Southeast Asia*, Report of the Senate Joint Foreign Affairs, Defence and Trade References Committee, Canberra: Senate Printing Unit, August 2004 (hereafter "JFADT Report"), p. xvii

on man", seeking and tracking identified perpetrators of crime.[15] Information-sharing difficulties abound: intelligence agencies are unwilling to let covert intelligence material be used in making criminal cases against the perpetrators of transnational crimes, while police won't allow evidence crucial to an ongoing investigation be passed outside the bounds of the investigation. Often police and intelligence agencies fail to realize they have information that is valuable to each other.

Another charge levelled at Australian intelligence agencies, and also their counterparts in the United States and the United Kingdom, was that their judgements about Iraq's WMD capabilities represented a failure of critical thinking. Intelligence assessment agencies, faced with uncertain and incomplete intelligence on Iraq's WMD activities, inferred from Baghdad's patterns of past weapons acquisitions and extensive attempts to avoid arms inspections that Iraq had WMD which it was trying to preserve and conceal. This was a judgement that came under extensive scrutiny after ISG inspections failed to find any WMD in Iraq after the war. The Flood Report argued that in the Australian agencies there was "a failure rigorously to challenge preconceptions or assumptions about the Iraqi regime's intentions" and more broadly "little evidence of a consistent and rigorous culture of challenge to and engagement on intelligence reports from collectors, and limited evidence of dialogue on assessed material."[16] Given the prominence of "groupthink" or "cognitive dissonance"-type explanations in many scholarly discussions of intelligence failures,[17] public critics also emphasized closed minds and lack of critical thinking in the AIC.[18] With the luxury of hindsight, various inquiries offered alternative explanations for Saddam's concealment activities: from bluff and national pride,[19] to brinkmanship and miscalculation,[20] to the paranoid and chaotic politics of dictatorship.[21] Intelligence analysis, like any interpretive activity, is prone to what Robert JERVIS calls 'the parochialism of the expert', where long experience and detailed knowledge give added certainty and a degree of uncontestability to judgments.[22] In the case of Iraq's concealment activities, the initial assessment led to a circular process of collection and analysis, as more and more intelligence on Iraq's concealment activities was collected after late 2002, in turn serving to firm up

---

[15] 9/11 Commission Report, p. 268

[16] Flood Report, pp. 25-6.

[17] For example, Irving L. JANIS, *Victims of Groupthink : A Psychological Study of Foreign-Policy Decisions and Fiascoes*, Boston: Houghton Mifflin, 1972; Roberta WOHLSTETTER, *Pearl Harbor : Warning and Decision*, Stanford: Stanford University Press, 1962

[18] See Paul MONK, "Why Didn't We Think of That?", *Australian Financial Review*, 2 November 2001; Lee CORDNER, "Reaping the Rewards: Executive Expectations of the Intelligence Investment", *Future Directions International*, May 2003, p. 3.

[19] PJCAAD Report, p. 80

[20] Flood Report, p. 23

[21] Butler Report, p. 15

[22] Robert JERVIS, 'What's Wrong with the Intelligence Process?', *International Journal of Intelligence and Counter-Intelligence*, Vol. 1, 1986, pp. 31-2.

judgments that these activities signified the existence of WMD.[23] This also points to another danger: as analysts have to devote increasing amounts of their time to digesting growing inflows of intelligence, there can be a tendency to start to think that the patterns emerging in the covert intelligence constitute the whole picture, when in reality covert intelligence can only provide a partial picture provided by the sources collection agencies can access and recruit. There is also an attendant danger in "fetishising" covert intelligence as inherently more valuable and indicative than other types of information.[24]

The final familiar charge leveled at the AIC is that due to its close intelligence relationship with the United States and United Kingdom, it acted as an uncritical cipher in dragging Australia (again) into "other peoples' wars".[25] It has long been charged that the UKUSA intelligence community architecture, which connects the United States, United Kingdom, Canada, Australia and (formerly) New Zealand in an intimate intelligence-sharing relationship, is a major conduit for the "colonization" of Australia's strategic thinking by its great power allies.[26] One commentator observed that there were "similar exaggerations and errors" in the Australian, American and British cases for war, leading to the strong implication that the AIC had simply regurgitated "previously digested US and British [intelligence] material" for the government.[27] Taking these charges seriously, the Parliamentary Committee Inquiry into Iraq's WMD scrutinized what it called the AIC's "external independence — that assessments are [driven by] Australia's national interest, independent of the interests of other nations."[28] Because of the geographic specializations of the UKUSA partners and the smaller size of the AIC, perhaps 97 per cent of the raw intelligence on Iraq's WMD was sourced from American and British collectors. As the Flood Report observed, it is "difficult for analysts to query and challenge foreign-sourced material … in general, source descriptions were less than helpful for analysts, tending to be selected from a small group of standard phrases."[29] Australian agencies also kept a close watch on American and British judgments about Iraq's WMD and links to AL QAEDA. Yet these elements do not necessarily lead to the conclusion that Australian assessments simply parroted those of their American and British counterparts. Both the Parliamentary Committee and the Flood Inquiry found that Australian agencies had been "much more measured" than those in Washington and London about Iraq's WMD capabilities. Australian agencies, for instance, rejected American claims about Saddam's links to AL QAEDA and British claims about Iraq's ability to deploy WMD within 45 minutes. Such small but significant differences among the allies suggest that the AIC took seriously its role of critically evaluating raw intelligence

---

[23] Butler Report, p. 89.

[24] WESLEY, "Analysing Transnational Intelligence", p. 102

[25] See Peter MANNING, "A Colonial State of Mind", *Griffith Review*, 5, Spring 2004

[26] See for example Joseph A. CAMILLERI, *ANZUS : Australia's Predicament in the Nuclear Age*, Melbourne: Macmillan, 1987

[27] Geoffrey BARKER, *Sexing It Up: Iraq, Intelligence and Australia*, Sydney: UNSW Press, 2003, p. 79.

[28] PJCAAD Report, p. 44.

[29] FLOOD Report, p. 25.

received and coming to independent judgments based on that material. That Australian agencies were not simply postboxes for passing on American and British assessments was demonstrated by a furore that developed in mid-2003, when they were roundly criticized for failing to pass on to the government US Bureau of Intelligence and Research (INR) doubts about intelligence reporting Iraqi attempts to source uranium from Africa.[30]

New Problems

The Parliamentary Joint Committee Inquiry into Intelligence on Iraq's WMD found that ONA's judgments on Iraq's WMD changed in tone almost overnight in mid-September 2002, when it began making "statements [on Iraq's WMD capacities] in the indicative rather than the subjunctive mood, thereby denoting greater culpability on Iraq's part and certainty on the part of the analysts."[31] The event causing ONA's enunciation of more definite judgements on Iraq's WMD was, it was implied, a request made by the office of Foreign Minister Alexander DOWNER for a document compiling unclassified information on Iraq's WMD activities. This led to a storm of accusations of "politicisation" of the AIC. The Flood Report defined politicization as relating both to the content of what is reported, and to what is not reported. In the former case, there is potential for either overt pressure from government or policy departments to reach a particular judgement, or an unconscious identification by the analyst with a particular policy outcome. In the latter case, analysts and managers may choose, either consciously or unconsciously, not to report on a particular issue of potential sensitivity for government.[32]

Critics identified politicization occurring in the AIC as a result of the involvement of heads of intelligence agencies on Prime Ministerial travels,[33] and in meetings of the National Security Committee of Cabinet,[34] or as the outcome of populating AIC management ranks with "politically astute" careerists from policy departments[35] who believe that their "career prospects [are] not enhanced by giving Ministers unpalatable advice or giving them information they did not want to hear."[36] Others claimed that ONA had allowed its concern with policy relevance to slip into policy advocacy, meaning selectively reporting or shaping intelligence to provide the appearance that a

---

[30] "Australian Intelligence Agency Admits It Did Not Tell Government of US Doubts Over Iraqi Evidence", Associated Press, 10 July 2003; "The PM and the Public Service", *Sydney Morning Herald*, 15 July 2003; Allan BEHM, "How We Got Iraq's WMDs Wrong", *The Australian*, 14 July 2003

[31] PJCAAD Report, p. 33

[32] Flood Report, p. 105

[33] Tom ALLARD, "The War of Secrets", *Sydney Morning Herald*, 6 March 2004

[34] Allan GYNGELL, "Closer Ties That Weaken the System", *Sydney Morning Herald*, 24 February 2004

[35] Andrew WILKIE, "A Lack of Intelligence", *Sydney Morning Herald*, 31 May 2003

[36] BARKER, *Sexing It Up*, p. 73; see also Philip KNIGHTLY, "Deadly Secrets", *The Bulletin*, 122, 27 April 2004; Tom ALLARD, "Canberra Was Warned on Spy Reports, Says Ex-Analyst", *Sydney Morning Herald*, 27 May 2003.

certain policy is working or appropriate despite evidence to the contrary.[37] Some critics accused the AIC of not enough involvement in the policy process, implying it is the role of intelligence assessments to "challenge, confront, question [and] dissent from conventional Departmental wisdom,"[38] or arguing that the AIC's fault was in "failing … to induce policy makers to learn,"[39] or that "If the decision maker, in this case the head of government, refuses to accept and act on vital intelligence, then intelligence officials have failed."[40]

The issue of the blurring of intelligence and policy roles goes to the heart of a foundational organizing principle of the AIC. The Hope Report, which in 1977 recommended the establishment of ONA and the formalization of co-ordination and oversight mechanisms for the AIC, quoted Walter Lippmann's advice: "The only institutional safeguard [guaranteeing the objectivity and impartiality of analysis] is to separate as absolutely as it is possible to do so the staff which executes from the staff which investigates. The two should be parallel but quite distinct bodies intrinsically uninterested in each other's personal success." To the outside, the process of intelligence analysis slipping from policy-relevant but objective reporting to producing reports that are anticipated to please Ministers and support their policies looks intuitively simple, even inevitable. If irrelevance leads to marginalization, then surely "the pressures to tell policy-makers what they want to hear can become irresistible."[41] Yet care should be taken in leaping to such judgements. Democratic government is by nature risk-averse: given the political costs that can attend a policy mistake or a proven failure to take indications of an emerging danger seriously, the process of government is prepared to endure significant short-term costs to allay the possibility of a long-term risk. By their nature, intelligence agencies are intended to warn governments of emerging risks. In an age of growing media and parliamentary scrutiny into what governments did and knew, there is a greater danger for intelligence agencies and personnel in failing to report significant risks or evidence of policy shortcomings than there is in telling ministers what they don't want to hear. No intelligence manager would last long if it came to light that he or she had glossed, ignored or refuted without good reason a development that could seriously affect the success of government policy. If the name of the game for intelligence is to capture ministerial attention, the presentation of discomforting or warning information, if adequately justified, will be much more compelling than merely presenting evidence for a policy's wisdom and effectiveness. And a government which by design or acquiescence allows its intelligence agencies to slide towards policy advocacy risks depriving itself of a purpose-built mechanism for warning about impending dangers or policy failures. Intelligence agencies must remain policy-relevant — understanding which issues are important to the government, where more information would assist in reaching decisions, and how intelligence product is used to shape decision-making and policy outcomes. Their role should then be to report

---

[37] See "ONA's Independence is Part of a Delicate Balance", *Sydney Morning Herald*, 15 April 2004

[38] Gary KLINTWORTH, "Flood Report: Mild Applause", *Asia Pacific Defence Reporter*, September 2004, p. 12

[39] Paul MONK, "Learning to See", *Griffith Review*, 5, Spring 2004

[40] CORDNER, "Reaping the Rewards", p. 3

[41] Desmond BALL, "Silent Witness: Australian Intelligence and East Timor", *The Pacific Review*, 14:1, 2001, p. 36

to government what the intelligence available suggests about the wisdom, sustainability and effectiveness of the policy. Against this background, charges of politicization of the AIC are serious indeed, and would require much more evidence than the apparent failure of judgment over Iraq's WMD. Though dismissed by critics as an inevitable finding by a government "insider", the Flood Report's finding that there was no evidence of politicization of the AIC is justified.

A related issue of controversy was the public use of intelligence by government. This development had occurred earlier in Australia than in the United States or United Kingdom, when Prime Minister John Howard explicitly cited an ONA Report to support the government's case against asylum-seekers just prior to the November 2001 federal election. Then, in the lead-up to the Iraq War, although the Australian government didn't use intelligence material in public presentations as its allies in Washington and London did, it referred repeatedly to intelligence in publicly making the case for war. In mid-September 2002, the office of Foreign Minister Alexander Downer requested an unclassified document listing intelligence indicating Iraq's possession of WMD capacity. As the Butler Inquiry commented in the British context, these developments were unprecedented in the direct use of intelligence to justify policy and in the commissioning of intelligence agencies to produce documents either for public release or as the basis for ministerial statements.[42] Two major criticisms were made of the Australian government's public use of intelligence. First, it was argued that the authority and objectivity of the AIC was being misused to bolster the government's position. Of particular concern were government assertions that the intelligence agencies had "cleared" ministerial statements on the case for the war in Iraq. When it emerged in the PJCAAD Inquiry that ONA had focused only on the accuracy of specific references to intelligence, the Committee reacted angrily to the government's casuistry:

"Accuracy must also encompass whether the picture being presented is complete. Ignoring significant elements of fact or opinion when citing intelligence assessments can have a distorting effect. A true and accurate interpretation must consider the total balance of the point of view being adduced in support of a policy.[43]"

By misusing intelligence in this way, the government risks undermining "public confidence in the value of intelligence and its credibility."[44] Second, there was concern that, by being forced from an intelligence reporting context into a public information one, the AIC had abandoned accuracy in favour of coherence and digestability. When writing for public consumption, it was suggested, the imperative is to highlight judgements rather than the detail and uncertainties of the evidence. This was the implication of the PJCAAD Report, which dated — without citing any evidence of causality — ONA's downplaying of the uncertainties and gaps in the intelligence on Iraq's WMD capacities from the preparation of the unclassified intelligence file for the Office of the Foreign Minister. Thus the public use of intelligence bolstered the charges of politicization of the AIC.

---

[42] Butler Report, p. 76

[43] PJCAAD Report, pp. 93-94.

[44] *Ibid.*, 74

The temptations for governments to use intelligence publicly are unlikely to abate. In an era of transnational threats, which by their nature emerge unlooked for, the new security imperative is to act to prevent such threats materializing. As British Prime Minister Tony BLAIR told American President George W. BUSH at a meeting in Crawford, Texas in April 2002, to allow threats to develop through inaction or inattention "would be to ignore the lessons of 9/11."[45] Yet in democracies, the public must still be provided with a rationale for policy, even if the motivations for the policy are not apparent. In this situation, intelligence is bound to be used to bolster the case for action. BLAIR told the Butler Inquiry in the United Kingdom that "the purpose of the [publicly released British intelligence] dossier was simply to say 'this is why we think this is important ... here is the intelligence that means this is not a fanciful view on our part, there is a real issue here."[46] Here the line is thin between providing the electorate and opposition with a common, objective corpus of intelligence on which they can judge the wisdom of alternative policies, and using intelligence to bolster public support for government policy. Shadow Australian Foreign Minister Kevin RUDD accused the government of sliding towards the former in "cherrypicking" from intelligence assessments only those judgements that supported its case for war.[47] Here governments face a risk that if they are perceived to be misusing intelligence, or skewing it to partisan purposes, or if the intelligence they use proves inaccurate, it will devalue the authority of intelligence over time, and impede their ability to use it to explain policy actions against transnational threats.

3. The Reforms

While the familiar intelligence failures generated pressures to increase the proficiency of the AIC, the newer problems produced concerns over its probity. Taking these issues into account, the recent reforms have had three basic effects on the AIC: they have reinforced the organizing principles of the AIC while overhauling its co-ordination mechanisms; upgraded external oversight of the AIC; and increased the resourcing and size of most of the intelligence agencies.

Functional Differentiation and Co-ordination

In the face of evidence of "horizontal" intelligence failures – inappropriate scrutiny of sources, "compartmentalisation" of intelligence and warning roles, insufficient contestation of judgements – some commentators suggested following the American lead and merging the AIC and law enforcement agencies into a new national security department. This became the policy of the Opposition Australian Labour Party. But the Flood Report and the government rejected such radical restructuring, opting instead to reassert functional differentiation in areas where it had become blurred, and instead strengthen the AIC's co-ordination mechanisms.[48] In his Report, FLOOD argued that "The clarity of the role played by each agency in the Australian Intelligence Community,

---

[45] Quoted in the Butler Report, p. 71.

[46] Quoted in *ibid.*, p. 77

[47] Quoted in Cynthia BANHAM, "Report is Proof of Deception", *Sydney Morning Herald*, 2 March 2004

[48] Verona BURGESS, "Ruddock Rejects Mergers", *Australian Financial Review*, 11 May 2005

together with minimal duplication of capability, is one of the strengths of the Australian system."[49] Here was also a statement that the AIC was not affected by the type of information-sharing problems experienced in the United States,[50] or the United Kingdom,[51] and that part of the reason for this was the AIC agencies' clear sense of functional specialization and interdependence. There is a strong feeling inside the AIC that different intelligence functions require different organizational cultures. The main reassertion of functional differentiation occurred in deconflicting the roles of the two assessment agencies, ONA and DIO. The latter's remit was carefully pruned to intelligence analysis in support of the Department of Defence and the Australian Defence Force's requirements, while ONA's role as the "peak national foreign intelligence assessment agency" was "reasserted". FLOOD and the government rejected criticisms that such deconflicting removed a much needed source of contestation of intelligence judgements from the AIC, instead arguing that fostering a culture of debate and challenge internally to ONA and DIO is a more efficient use of resources.

The counterpart to reinforcing functional differentiation was to improve intelligence co-ordination. Co-ordination mechanisms have been forged at all levels. At the lowest level, Australia followed the United States and the United Kingdom in establishing a joint, 24-hour, all-source terrorist threat centre, termed the National Threat Analysis Centre (NTAC). Housed in ASIO, NTAC is staffed by secondees from all of the AIC agencies, plus the AFP, DFAT and the Department of Transport and Rural Services. It is acknowledged as the authoritative source of threat advice, and plays a regular role in DFAT's preparation of Travel Advisories. At a higher level, the FLOOD reforms resulted in the creation of the Foreign Intelligence Co-ordination Committee (FICC), and the strengthening and better resourcing of the roles of ONA and its Director-General as co-ordinators of the AIC. The FICC formalizes a committee that had developed informally, known as the Heads of Intelligence Agencies Meeting (HIAM), in gathering together for a monthly co-ordination meeting the heads of all AIC agencies and the AFP, plus senior representatives from DFAT and the Departments of Prime Minister and Cabinet (PM&C). Chaired by the Director-General of ONA and resourced by a Secretariat within ONA, the FICC deals with co-ordination, strategic planning and evaluation within the AIC. The FICC has been provided with a formal interface with the policy process through its relationship to the newly created National Security Division within PM&C, and through the Secretaries' Committee on National Security (SCONS) to the National Security Committee of Cabinet (NSCC). All of these mechanisms are intended to serve the functions of making sure the whole of government is more responsive to intelligence issues, and that intelligence judgements are more closely integrated into government policy-making.

The Australian government has been able to adopt such a relatively minimalist approach to horizontal co-ordination issues due to the AIC's small size and established culture of collegiality. The new, formal co-ordination mechanisms are assisted by long-established understandings of roles and responsibilities. The regular drawing of AIC managers from DFAT and the Department of

---

[49] Flood Report, p. 69

[50] 9/11 Commission Report, p. 353

[51] Butler Report, p. 111

Defence, so often criticized as resulting in the "dumbing down" and de-professionalization of the AIC, has brought a culture of practical co-operation among the senior managers of the intelligence agencies. This commitment at senior levels drives co-operation at lower levels, ensuring a much more rigorous, judicious and collaborative approach to intelligence collection tasking and feedback; it also helps allay collectors' concerns about the instrusiveness of too rigorous a process of co-ordination and oversight. So important is the "hidden lubricant" of co-operation within the AIC that many worry that the growth and professionalization that will follow the Flood reforms will threaten the community's culture of easy collegiality.

External Oversight

A series of scandals involving Australia's intelligence collection agencies over the years has resulted in the steady strengthening of external oversight mechanisms. The main innovations have been the creation of the Parliamentary Joint Committee on ASIO, ASIS and DSD and the Inspector-General of Intelligence and Security (IGIS), a statutory office with the responsibility to investigate and report regularly on the collection agencies' operations and probity, with the ability to initiate investigations into collection agencies, and with the powers of a royal commission. The PJCAAD and IGIS have both played a prominent role in recent years in assessing the propriety and proficiency of the agencies of the AIC.

The Flood Report took the charges of politicization of the AIC seriously. Although it cleared Australian intelligence agencies of charges of politicization, it acknowledged their need to preserve their reputation for rigour and objectivity: "The functioning of Australia's intelligence agencies is a matter of great public interest and scrutiny." While conceding that foreign intelligence assessment agencies rarely threaten the rights or privacy of Australian citizens, FLOOD argued that extending parliamentary oversight to ONA and DIO "would enhance confidence in the Parliament and the public that the full range of intelligence agencies is accountable to a senior group of parliamentarians," and recommended a concomitant name change to the Parliamentary Joint Committee on Intelligence and Security (PJCIS). With a similar logic, the Flood Report recommended extending the remit of IGIS to include ONA and DIO, including giving IGIS the capacity to initiate inquiries at his or her own discretion into the analysis agencies' activities, and in particular periodically reviewing ONA's statutory independence.

While the intentions of these reforms are laudable, it is difficult to see how they will work in practice without compromising the capacities of the analytical agencies to make hard, objective judgments. FLOOD seemed to recognize the dangers of exposing analytical agencies' judgements to regular parliamentary review when he suggested that "Just as the advice that officials provide to Ministers is not disclosed in Senate Legislation Committee hearings, the judgments of assessment agencies should not be subject to parliamentary scrutiny." Rather, in addition to parliamentary review of ONA's and DIO's "budgetary and administrative matters", "the process by which ONA and DIO produce their assessments is an area which could be open to parliamentary scrutiny."[52] It is hard to

---

[52] Flood Report, p. 58

see how a parliamentary committee will be able to confine itself to these matters. As the practice of Senate Estimates Committee hearings shows, remits to scrutinize "budgetary and administrative matters" are routinely overstepped. And it will be impossible properly to review the process by which assessments are produced without having some idea of what those assessments were. Added to these concerns are growing doubts that parliamentary committees can act as impartial overseers, with many commentators noting the increasingly bitter partisan divisions that are characterizing debates over issues of security and intelligence.[53] The inherent subjectivity of reviewing the process and outcomes of assessment processes is itself revealed in discrepancies in the two reviews on Iraq WMD: while the PJCAAD dated a hardening of ONA judgments from mid-September 2002,[54] the Flood Report claimed that these changes did not occur in ONA Reports until early 2003.[55] Faced with the possibility of partisan politics and subjectivity tainting the parliamentary review process, it is hard to see how intelligence assessment agencies will not start to factor in possible future parliamentary scrutiny when making their judgments. The danger is that the result will be a tendency to be more cautious and qualified in assessments, the very charges that many critics have argued result from the politicization that these oversight reforms are intended to address.

Resourcing and Expansion

Over many years, there has developed in Australia's security and intelligence institutions a preference for maintaining small but very high-quality capabilities. The Australian Defence Force is by regional standards a small military organization, yet it takes pride in its very high levels of training and advanced technology. The AIC has similarly remained much smaller than the intelligence communities of its closest allies — the United States spends 100 times the amount Australia spends on intelligence; Britain spends four times Australia's amount. Partly, the AIC has been able to afford the luxury of being small because it is conscious that it is a part of the most powerful intelligence-gathering collaboration in the world, the UKUSA agreement. The focus of Australia's intelligence collection efforts is clearly spelled out in the Flood Report: "On Southeast Asia and the South Pacific, Australia needs to be a global leader in intelligence … Australia's intelligence on North Asia should be exceptionally good … Intelligence on South Asia should be very good,"[56] implying that for intelligence on other regions, Australia is able to rely on its UKUSA partners. In terms of analysis, FLOOD argued that "Australia needs to maintain an independent capacity across the whole spectrum of issues on which the government needs advice. Australia must be able to critically assess intelligence sourced from others."[57]

---

[53] See for example Carl UNGERER, "Issues in Australian Foreign Policy: January to June 2004", *Australian Journal of Politics and History*, 50:4, 2004

[54] See PJCAAD Report, p. 33

[55] See Flood Report, p. 29

[56] *Ibid.*, pp. 12-13

[57] *Ibid.*, p. 15

Working under the political imperative to leave no stone unturned in protecting Australia from transnational threats, the government had begun to expand the budgets and powers of the frontline collection agencies in 2001. Australia's spending on foreign and security intelligence increased from $332 million in 2000-2001 to $659 million in 2004-2005, before the adoption of the Flood Report reforms, with the vast majority of that increase going to ASIO, ASIS and DSD. Staff levels in ASIO and ASIS have or are projected to double in the coming years.[58]

The analytical agencies' preference for "boutique" capabilities came under sustained pressure during the controversies and inquiries. Parliamentary committees appeared genuinely astonished at how few analysts ONA had to deal with the growing amounts of intelligence received on issues such as Iraq and terrorism. The PJCAAD learned that ONA had two analysts with Middle East expertise and one with strategic analysis expertise working on Iraq's WMD capacities, and that "their focus was not exclusively on Iraq during this time."[59] FLOOD recommended a doubling of ONA's staff from 74 to 145 and a budget increase from $13.1 million to $25 million per annum. He also recommended transferring the Open Source Unit from DFAT to ONA, a move which acknowledges open-source information as important intelligence, which responds to the growing emphasis on open-source information among Australia's intelligence allies, and which will systematize the mining and use of open-source information and harmonize it with the tasking of covert intelligence collection.

Faced with such a sudden expansion in budgets and personnel, questions have been raised about the AIC's ability to find suitable recruits while maintaining standards, and to "digest" such large numbers of new staff.[60] Generally, managers in intelligence agencies report that, contrary to media reports, applications have surged since September 11, benefiting from greater public interest in the intelligence community. Apart from certain language and technical skills, there has been little or no problem filling positions at more junior levels. The AIC has instituted a common process of security vetting and a common induction course for new recruits to all agencies. At more senior levels, or for certain skills sets, some agencies have found that their location in Canberra, away from the country's major population centres, has hampered their ability to attract appropriate staff. Some agencies have run into problems arising from a shortage of mid-level managers with broad intelligence experience who are able to manage and mentor new staff and provide quality control. In areas of skills shortages, there has been some competition among agencies, but this has been managed collegially. The heads of the AIC agencies recognize that some staff mobility among agencies builds communication links and increases the stock of mutual understanding in the community.

4. Conclusion

The recent changes to the AIC have reinforced, rather than challenged, the basic organizing

---

[58] "Australia Doubles Spy Agency", SBS World News Headline Stories, 17 October 2005

[59] PJCAAD Report, p. 47.

[60] See for example Julie MACKEN, "I Spy a Problem on Intelligence", *Australian Financial Review*, 24 November 2005; Deborah Snow, "A Shortage of Spooks", *Sydney Morning Herald*, 15 November 2004

principles according to which it has always operated. The judgments of various inquiries and the government seem to have been that, if properly resourced and co-ordinated, the AIC should be able to cope adequately with emerging challenges and rectify past failings. It is too early to judge whether these judgments, and the reforms they have entailed, are indeed adequate to cope with the challenges posed by transnational threats, or the seemingly recurring "familiar" problems with intelligence processes, or especially the political pressures on intelligence agencies. If these challenges are too great to be solved by minor structural changes and resourcing upgrades, the next round of major reforms to the AIC may be closer than a quarter century away.

Professor Michael WESLEY is the Director of the Griffith Asia Institute at Griffith University, Australia. Prior to taking up this position in July 2004, he was the Assistant Director General for Transnational Issues at the Office of National Assessments. Before he joined ONA, he was a Senior Lecturer in the School of Politics and International Relations at the University of New South Wales and a Research Fellow at the Asia-Australia Institute, also at UNSW.

Non classifié
Avril 2006
N° 88

Service canadien du renseignement de sécurité

Commentaire

Probité et compétence : défis et changements au sein de l'appareil australien du renseignement

Michael Wesley

La publication de *Commentaire* a pour objet de stimuler un débat public sur des questions rattachées à la sécurité nationale.

1. Introduction

L'appareil australien du renseignement (AAR) semble soumis à d'importants changements tous les vingt-cinq ans. Les principaux organismes de collecte de renseignements, c'est-à-dire l'ASIS (Australian Secret Intelligence Service), le service responsable du renseignement extérieur, le DSD (Defence Signals Directorate), l'organe chargé de la sécurité électronique, et l'ASIO (Australian Security Intelligence Organisation), l'organisation responsable du renseignement et de la sécurité, ont tous été créés à la fin de la seconde guerre mondiale. Puis, à la fin des années 1970, le Commonwealth a formé au sein de l'ONA (Office of National Assessments) le bureau des évaluations nationales, un nouvel organisme d'analyse et de coordination des renseignements indépendant de la DIO (Defence Intelligence Organisation), l'organisation qui regroupe les divers services secrets militaires, et officialisé les principes d'indépendance fonctionnelle et de surveillance. Puis, jusqu'en 2004, cette structure a largement échappé aux réformes organisationnelles imposées aux autres organismes d'État. Cette année-là, un nouveau train de réformes a été adopté en réponse à de nouvelles pressions, aux controverses, aux enquêtes et aux rapports d'enquête. Les activités quotidiennes de l'AAR et chacune des étapes de la vaste restructuration dont il a fait l'objet ont été guidées par trois grands principes structurants : la spécialisation fonctionnelle des services de collecte de renseignements, le cloisonnement des activités de collecte et d'analyse, d'une part, et des activités de collecte et d'évaluation, d'autre part, selon qu'il s'agit du renseignement intérieur ou du renseignement extérieur. Récemment, alors que certains des plus proches alliés de l'Australie envisageaient de restructurer leurs appareils du renseignement respectifs, Canberra optait plutôt pour des réformes plus modestes qui, loin de contester la validité de ces principes, les ont plutôt confirmés et renforcés.

Les plus récentes réformes de l'AAR sont attribuables à deux ensembles de circonstances connexes. Dans un premier temps, l'accélération de la mondialisation modifie la nature, le nombre et l'urgence des demandes que reçoivent les services de renseignement d'État. Si les avantages de ce phénomène ont été vantés tout au long des années 1990, il faudra sans doute chercher en priorité, au cours de la première décennie du XXIe siècle, à composer avec ses aspects les plus sombres. Dans un second temps, l'AAR a été la source de plusieurs controverses très médiatisées. En 1999, les services secrets militaires ont été accusés d'avoir ignoré des renseignements sur les activités des milices du Timor oriental, soutenues par l'Indonésie, et de ne pas les avoir communiqués aux unités de campagne des forces de défense australiennes et aux plus proches alliés de l'Australie. Le scandale s'est amplifié quand un officier de liaison du renseignement militaire australien en poste à Washington s'est suicidé. En 2004, les accusations précédentes ont été évoquées à nouveau, au milieu des nouvelles controverses qui éclaboussaient l'appareil du renseignement. En 2001, l'ONA a essuyé les critiques après avoir inventé des renseignements à l'appui de la prise de position du gouvernement sur les actions des demandeurs d'asile, tandis que la DSD a été accusée d'avoir mis illégalement sur écoute des citoyens australiens qui défendaient les demandeurs d'asile. En 2002, après les attentats de Bali dans lesquels 88 Australiens ont perdu la vie, des voix se sont élevées pour demander si les services de renseignement australiens avaient pris suffisamment au sérieux la menace que représentent les groupes islamistes violents en Asie du Sud-Est. Enfin, l'AAR a de nouveau longuement attiré

l'attention sur lui en 2003 après avoir fourni des arguments à l'appui de la participation de l'Australie à l'invasion de l'Irak en mars de cette même année.

Il en a résulté une série d'enquêtes spéciales et parlementaires sur la compétence de l'AAR et ses opérations. Comme elles se sont déroulées au moment où l'invasion de l'Irak faisait l'objet d'un âpre débat partisan, juste avant les élections fédérales de 2004, elles ont suscité un intérêt sans précédent pour les services de renseignement. Le processus d'examen a atteint son point culminant avec l'enquête, en 2004, de l'ancien directeur général de l'ONA, Philip FLOOD, qui a proposé au gouvernement vingt-trois mesures de réforme qui ont toutes été mises en oeuvre sauf une[1]. Le présent document examine les récents changements que le gouvernement australien a apportés au sein de l'AAR à la lumière des nouvelles pressions auxquelles sont soumis les services de renseignement et des accusations d'« incompétence » dont ils ont fait l'objet.

1. Pressions exercées sur les services de renseignement

Les services de renseignement de l'Australie, comme ceux de ses plus proches alliés, doivent relever deux grands défis qui découlent de la mondialisation. En un peu plus d'une décennie, celle-ci a transformé la nature des menaces qui pèsent sur les sociétés modernes, ainsi que les moyens dont disposent les services de renseignement et leurs cibles, et le contexte politique et diplomatique dans lequel évoluent ces services. Les menaces transnationales posent des défis complexes que la plupart des appareils du renseignement n'ont pas encore complètement relevés. En matière de sécurité, le terrorisme est l'une des grandes priorités nationales de la plupart des pays occidentaux, mais ceux-ci consacrent très peu de ressources aux autres défis transnationaux. L'Australie doit actuellement veiller, comme nombre d'autres pays, à ce que les services de renseignement ne consacrent pas trop de ressources à la lutte contre le terrorisme, au détriment de leurs autres cibles et activités. Tout pourrait changer si d'autres menaces transnationales frappaient autant les esprits que le terrorisme.

Défis transnationaux

La disparition des antagonismes issus de la guerre froide et la montée de la mondialisation ont hissé les menaces transnationales au premier rang des enjeux de sécurité nationale et, par voie de conséquence, des préoccupations des services de renseignement. Ces menaces peuvent être décrites comme suit : elles prennent naissance dans une ou plusieurs sociétés (et non au sein de la structure décisionnelle ou des ressources d'un État) et se propagent, ou sont imitées, au-delà des frontières nationales pour compromettre la sécurité ou ébranler les valeurs d'une autre société et, finalement, la sécurité ou l'existence même d'un État. Elles incluent le terrorisme, la prolifération sub-étatique des ADM et de la technologie des missiles, le crime organisé, la production et la distribution des stupéfiants, les pandémies graves, les mouvements de population anormaux, l'exploitation illégale

---

[1] Commonwealth of Australia, *Report of the Inquiry into Australian Intelligence Agencies, juillet 2004*, Canberra, Goanna Print, 2004.

des ressources et les mouvements doctrinaires perturbateurs[2]. La plupart de ces menaces émanent de réseaux transactionnels décentralisés formés d'acteurs non étatiques qui sont éparpillés aux quatre coins du globe et dont les contacts les uns avec les autres sont noyés dans la multitude des transactions effectuées chaque jour dans un univers mondialisé. Les liens qui se créent entre ces acteurs se définissent de plus en plus en termes d'objectifs généraux partagés ou d'intérêts communs dans une transaction donnée plutôt qu'en fonction de la loyauté ethnique ou familiale ou d'une structure de commandement officielle. En conséquence, les menaces transnationales les plus dangereuses auxquelles nous faisons face commencent à adopter une caractéristique connue sous le nom de « comportement émergent » en biologie, c'est-à-dire que les interactions dynamiques entre les agents face à des situations locales données induisent des comportements collectifs plus souples et plus complexes qu'une organisation centralisée et hiérarchisée ne peut adopter. La mondialisation des communications permet aux groupes isolés de se renseigner sur les techniques les plus efficaces utilisées ailleurs et de les adopter. Souvent, les flux transnationaux les plus dangereux ne concernent ni des gens, ni des biens, mais des informations – doctrine du jihad international, conception de centrifugeuses au gaz, production d'amphétamines synthétiques, de charges formées, etc.

Les menaces transnationales remettent en cause la définition traditionnelle de sécurité et de relations internationales. Des pays comme l'Australie se sont rendus à l'évidence : les principales menaces contemporaines n'émanent plus d'autres États et ne visent plus leur puissance militaro-industrielle ou leurs institutions. Les menaces transnationales – terrorisme, criminalité, stupéfiants, pandémies, etc. – , ébranlent les fondements et les règles mêmes de la société civile sur lesquelles repose l'organisation sociale moderne. Non seulement la mondialisation favorise-t-elle une diffusion plus rapide et plus large que jamais auparavant des menaces transnationales, mais elle amplifie ce qu'Émile DURKHEIM appelle l'« organicisme » croissant des sociétés modernes, c'est-à-dire l'interdépendance grandissante des acteurs et des institutions et la spécialisation accrue de leurs fonctions[3]. Cette spécialisation croissante et les modes d'interaction observés au sein des sociétés modernes, la dépendance croissante de celles-ci envers les technologies de l'information, leurs méthodes de production et leurs systèmes de stockage « juste à temps », ainsi que leur impatience croissante face à la redondance ont lourdement aggravé leur vulnérabilité aux pannes catastrophiques[4]. Les menaces transnationales contribuent dès lors à brouiller la distinction qui existe entre, d'une part, collecte de renseignements sur le territoire national et à l'étranger et, d'autre part, sphère publique ou d'État et sphère de sécurité privée ou sociétale[5]. Le rôle des services de

---

[2] Michael WESLEY, *Analysing Transnational Intelligence*, in *New Frontiers of Intelligence Analysis*, Carole DUMAINE et L. Sergio GERMANI (éditeurs), Actes de conférence, Sherman Kent School for Intelligence Analysis, 2004.

[3] Emile DURKHEIM, *De la division du travail social*, New York, Free Press, 1984.

[4] Michael WESLEY, « Towards a Realist Ethics of Intervention », *Ethics and International Affairs*. La question a été examinée sous un angle plus polémique par Ulrich BECK dans *Société du risque. Vers une nouvelle modernité*. Traduit par Mark RITTER, Londres, Sage Publications, 1992.

[5] Gregory F. TREVERTON, « Remodeler le renseignement pour le partager avec " nous-mêmes " », *Commentaire du SCRS*, n° 82, été 2003, p. 5.

renseignement extérieur, qui sont chargés de recueillir des renseignements sur l'étranger et de les analyser, a profondément changé. En effet, au lieu de se concentrer uniquement sur la recherche de renseignements sur les intentions et les moyens des autres États, ils ont été amenés à empiéter de plus en plus sur le territoire de leurs homologues des services de sécurité intérieure et à s'intéresser aux activités, aux intentions et à l'influence d'individus et de groupes susceptibles de menacer un jour la vie et les moyens de subsistance des Australiens. Et comme les menaces transnationales s'ajoutent à celles qui planent déjà sur la sécurité des États, d'autres organismes gouvernementaux sont amenés à s'intéresser à la question de la sécurité nationale et à consommer et à recueillir des renseignements. La vulnérabilité des sociétés et de leurs infrastructures aux attaques terroristes a entraîné l'inclusion des ministères responsables de l'immigration, de la santé et des transports dans les structures sécuritaires et les informations dont disposent leurs réseaux administratifs, jugées vitales, sont intégrées dans les systèmes d'alerte rapide des services de renseignement.

Compte tenu de leur nature et de leur nombre, les menaces transnationales posent d'énormes difficultés aux services de renseignement habitués à se concentrer sur les activités des États et de leurs agents. Les méthodes de travail classiques des services occidentaux ont été conçues à l'origine pour leur permettre de recueillir des renseignements sur quelques États secrets, mais très hiérarchisés et fortement centralisés, et de les interpréter. Il s'agissait en général de se renseigner sur des politiques, des décisions et des moyens qui évoluaient, en toute logique, dans le même sens pendant des dizaines d'années. Dans le cas des réseaux transactionnels décentralisés, il est particulièrement difficile de collecter des renseignements et de les évaluer, parce qu'il n'existe ni hiérarchie, ni structure de commandement claire. Dès lors, le véritable défi réside dans l'évaluation des renseignements obtenus. Tout rapport, quel qu'il soit, sur les intentions d'un ou de plusieurs acteurs d'un réseau transnational ne donne aux services de renseignement qu'une image très floue des intentions et des moyens de l'ensemble de ce réseau. Et comme les acteurs décentralisés adaptent constamment leur comportement aux circonstances locales, ils n'ont pas le loisir de tracer un portrait fiable du réseau. Tous les services, qu'ils collectent des renseignements ou les analysent, se heurtent à ces défis.

Les responsables de la collecte de renseignements sur les menaces transnationales doivent de plus en plus souvent analyser eux-mêmes, et sans tarder, les informations obtenues pour les valider et établir l'ordre de priorité des cibles auxquelles ils s'intéresseront au sein d'organisations en constante évolution. Les progrès des technologies de l'information et la diffusion accrue d'informations sur les méthodes des services de collecte de renseignements compliquent le travail de ces derniers. Les particuliers et les organisations peuvent maintenant se procurer, à faible prix, des technologies de chiffrement très performantes et utiliser une foule d'innovations offertes sur l'Internet pour assurer la confidentialité de leurs communications. Pendant que les organismes SIGINT font l'impossible pour rester à l'avant-garde de ces technologies et de ces astuces, les acteurs transnationaux ont recours à une foule de stratégies de faible technicité qui compliquent à leur tour le travail des responsables du renseignement humain (HUMINT) à la recherche d'indices de leurs activités. Comme les États sont de plus en plus présents à l'étranger, dans un effort pour prévoir et contrer les menaces transnationales, les services de renseignement consacrent de plus en plus de ressources au

soutien des opérations militaires et policières à l'étranger et de leurs propres actions perturbatrices plutôt qu'à la collecte de renseignements axée sur l'analyse. En outre, ces forces militaires et policières produisent d'importantes quantités de renseignements de grande valeur que les organismes de collecte et d'analyse doivent réunir et évaluer.

S'agissant de menaces transnationales, les organismes d'analyse sont engagés dans une lutte asymétrique. Aux yeux des terroristes et des criminels membres de réseaux décentralisés, tous les problèmes ont un caractère local et sont réglés localement; les services de renseignement, pour leur part, doivent s'efforcer de les comprendre dans leur intégralité. Tout l'art réside donc dans la capacité d'isoler et de prévoir les comportements et les possibilités plutôt que de chercher des réponses précises. Comme l'a expliqué un observateur, dans le cas des menaces transnationales, « la logique n'est d'aucune utilité dans la recherche de réponses à de nombreuses questions parce que celles-ci concernent des événements à venir, par exemple les intentions non encore concrétisées d'êtres humains ou des facteurs dont la présence simultanée relèvera du hasard »[6]. L'analyse des renseignements sur ces menaces est donc essentielle. Elle permet, d'une part, d'évaluer les signes avant-coureurs de nouvelles menaces et de faire rapport sur l'évolution stratégique des menaces transnationales et tend, d'autre part, à se transformer en analyse tactique au profit des opérations de maintien de l'ordre, ce qui alourdit considérablement la charge de travail des ressources limitées des organismes d'analyse.

Contexte politique et diplomatique

En créant un climat de peur au sein des populations et en imposant de nouveaux impératifs d'intervention aux gouvernements, les menaces transnationales ont également modifié le contexte politique dans lequel évoluent les services de renseignement. Depuis les attentats du 11 septembre 2001, surtout, ceux-ci ont troqué, dans l'inconscient populaire, leur rôle d'obscurs services « d'espionnage sur d'autres espions » pour celui plus « honorable » de protecteurs de la société, à l'image en quelque sorte des forces de défense et des organismes de maintien de l'ordre. Les nombreux reportages des médias sur les enquêtes sur les services de renseignement en Australie et ailleurs dans le monde et la pléthore de débats et de révélations sur le sujet, souvent faites par d'anciens agents mécontents, ont révélé l'existence de l'AAR au grand jour et renseigné la population sur ses pratiques. De nombreux professionnels du renseignement supportent mal, entre autres choses, que leurs services ne puissent répondre à bon nombre de leurs détracteurs, ce qui laisse la voie libre aux déformations et aux malentendus. Comme le budget et les pouvoirs des services de renseignement ont augmenté après le 11 septembre, le public s'attend inévitablement encore plus à ce que rien ne leur échappe. Les accusations répétées d'« incompétence » et la culture publique, qui a besoin d'un coupable à qui imputer la responsabilité des attentats terroristes, ont contré les tentatives des gouvernements de réduire ces attentes. Le public comprend encore très mal quelles sont les capacités et les limites des services de renseignement. Il faut mieux l'informer. Une majorité

---

[6] Lee S. STRICKLAND, « The Information Shortcomings of 9/11 », in *Information Management Journal*, vol. 38, n° 6, Novembre/décembre 2004, p. 43.

d'Australiens semble appuyer la participation des services de renseignement à la lutte contre le terrorisme, mais certains craignent que ce rôle ne soit le prélude à un État de sécurité nationale. Le vif débat qui a entouré la décision d'accorder des pouvoirs de détention et d'interrogation accrus à l'AAR a sensibilisé davantage la population aux garanties juridiques individuelles et le rôle prédominant des services de renseignement avant et après le déclenchement de la guerre en Irak a réduit la volonté de certains groupes et particuliers de coopérer avec eux.

L'impact du terrorisme sur la politique démocratique a grandement complexifié le contexte politique dans lequel évoluent les services de renseignement. En Australie, les effets psychologiques des attentats du 11 septembre se sont manifestés quand un nombre accru de réfugiés de la mer a soudain fait route vers le continent insulaire. Ils ont créé, ce faisant, un climat de menace insidieux dans le contexte duquel les responsabilités du gouvernement en matière de sécurité nationale et de gestion de l'économie nationale ont pris le pas sur toute autre considération dans l'esprit de la vaste majorité des électeurs. Les gouvernements, soucieux de « redorer leur blason » en matière de sécurité nationale, et les partis d'opposition, déterminés à « le ternir », ont élevé la sécurité publique au tout premier rang de leurs priorités politiques. Quand un climat de peur du terrorisme s'installe au sein de la population, rien ne doit être négligé, dans l'intérêt de la sécurité publique. Les services de renseignement et d'application de la loi, considérés comme les meilleurs remparts contre les menaces transnationales, se sont vu accorder des pouvoirs et des ressources accrus. Sur fond de rivalités partisanes axées sur la compétence en matière de sécurité nationale, les médias et les parlementaires étudient désormais la question beaucoup plus attentivement. Les partis d'opposition utilisent de plus en plus les comités parlementaires – plus particulièrement les audiences annuelles du comité du budget du Sénat –, pour interroger les chefs des services de renseignement sur les dossiers qui, à leur avis, érodent la confiance de l'électorat dans la gestion gouvernementale de la sécurité nationale. Les services de renseignement savent, tout comme leurs maîtres politiques, que chaque fois qu'un événement est mis sur le compte de leur « incompétence », leurs pratiques, leur méticulosité et leur jugement peuvent être et sont, de fait, soumis à l'examen minutieux des médias et des parlementaires, qui bénéficient évidemment de la sagesse qu'apporte la compréhension a posteriori des événements.

Dans un tel contexte, tout renseignement négligé ou mal évalué ou auquel il n'a pas été donné suite peut provoquer une crise politique. Les services de renseignement doivent veiller à communiquer toute information crédible sur une menace aux autorités politiques et la population s'attend à ce que celles-ci la lui transmettent sous forme d'avertissements à l'intention des voyageurs. Les services de renseignement, qui se retrouvent indubitablement en première ligne du dispositif de protection de la société contre les menaces transnationales, redoutent de ne pas interpréter correctement un renseignement qui les informe de l'imminence d'une menace. Devant une telle alternative – transmettre ou non un renseignement qui pourrait être authentique, aussi invraisemblable qu'il puissse paraître – , il est normal de le transmettre. Si les services d'analyse ne résistent pas à la tentation de réagir ainsi, l'évaluation des renseignements et la prise des décisions appropriées relèvera d'échelons de plus en plus élevés de l'appareil gouvernemental et leur existence même sera

remise en question. Les impératifs politiques qui découlent des menaces transnationales amplifient en outre les contraintes temporelles auxquelles sont soumis les services de renseignement, qui croulent sous les informations de qualité très variable. Ils doivent fournir en temps utile à leurs clients des renseignements de très grande qualité ainsi que des opinions et des prévisions fiables pendant que les informations sont encore « fraîches ». Les conclusions qu'ils tirent de leurs évaluations et de leurs analyses reposent inévitablement sur les informations disponibles à un moment bien précis et ils n'ont pas le loisir d'attendre une confirmation ou d'avoir une meilleure compréhension de la situation. Il en découle également que ceux qui recueillent les renseignements et ceux qui les analysent peuvent rarement prendre le temps de les vérifier. La masse de renseignements bruts que reçoivent les bureaux ministériels et les services des politiques – la situation perdurera sans doute, les ministères demandant toujours plus de renseignements et les services qui les recueillent cherchant sans cesse à accroître l'éventail de leurs clients –, n'a fait qu'accroître ce besoin d'analyses en temps réel, car ils exigent de plus en plus que la fiabilité des renseignements reçus soit établie rapidement. Qui plus est, les ministres australiens et leurs principaux conseillers sont aujourd'hui des consommateurs de renseignements beaucoup plus expérimentés et avertis – bon nombre d'entre eux administrent un portefeuille lié à la sécurité nationale depuis une dizaine d'années et se rencontrent régulièrement au sein du puissant NSCC, le comité du cabinet chargé de la sécurité nationale, pour discuter de dossiers étayés par des renseignements.

La montée des menaces transnationales a également entraîné les services de renseignement australiens dans le monde de la diplomatie. Même si, dans le domaine du renseignement, la logique antagoniste persiste toujours entre les États, la nature de ces menaces exige une plus grande coopération. L'inquiétude des pays avancés face aux « États déliquescents » – éléments faibles de la structure internationale où terroristes, criminels et proliférateurs s'installent et transitent –, est apparue au moment où ils ont entrepris de rassurer le reste du monde, et plus particulièrement les investisseurs et les touristes, sur leur engagement en faveur d'une saine gouvernance. Les menaces transnationales ont entraîné un échange accru de renseignements entre l'Australie et ses partenaires de l'alliance UKUSA, à savoir le Royaume-Uni, les États-Unis et le Canada, mais a érodé sa spécialisation géographique. Comme l'a déclaré un membre de la direction d'un service de collecte de renseignements, « nous ne pouvons plus nous contenter de surveiller notre cour arrière, ce n'est plus suffisant aux yeux de nos clients et de nos partenaires ». Les services de renseignement et d'application de la loi australiens ont été à l'avant-garde de la coopération régionale contre les menaces transnationales, en collaborant aux enquêtes de leurs homologues régionaux, en formant leur personnel et en participant à un réseau sans cesse plus étendu d'échange de renseignements et d'opinions sur ces menaces à l'extérieur du cadre des alliances traditionnelles. Les contraintes temporelles auxquelles sont soumises les ressources sont déjà sollicitées au maximum de ces organisations mises à part, la « diplomatie du renseignement » – et le partage des renseignements et de l'expertise qui en résulte –, fait naître des craintes au sujet de la protection des sources et des techniques ainsi que des conséquences de la coopération sur l'avenir du contre-espionnage dans ces États. Enfin, la multiplication des ententes de liaison a elle aussi généré un plus grand nombre de renseignements dont la fiabilité n'est pas établie et que les services spécialisés doivent analyser.

2. Défaillances des services de renseignement

Les services de renseignement australiens font l'objet d'une controverse depuis 1999, mais en 2004, deux questions surtout ont dominé les travaux des commissions d'enquête et le débat : l'AAR a-t-il sous-estimé et négligé la menace que représentait l'islamisme en Asie du Sud-Est avant les attentats à la bombe d'octobre 2002 à Bali et a-t-il exagéré la présence possible d'armes de destruction massive (ADM) en Irak avant l'invasion de mars 2003? Les enquêtes et la controverse ont porté, à peu de choses près, sur les mêmes sujets aux États-Unis (11 septembre et Irak) et au Royaume-Uni (attentats de Bali et Irak), et nombre des accusations, des arguments et des avis entendus en Australie ont été influencés par ce qui s'est passé dans ces deux pays. Dans les trois cas, les éléments à l'origine de la défaillance des services de renseignement ont été répartis en trois grandes catégories. La première comprend un éventail de situations liées à la collecte et à la communication des renseignements : surcroît de renseignements et mauvaise évaluation des sources, choix des cibles de la collecte de renseignements fondé sur des hypothèses et non-communication des informations aux autres organismes. La deuxième concerne le manque d'imagination : les idées préconçues ont inhibé la pensée créatrice ou encore les déductions « heuristiques »[7] ont empêché l'examen d'autres pistes d'explication. Enfin, la troisième catégorie regroupe les questions liées à la « politicisation »: les services de renseignement se sont-ils laissés influencer, ouvertement ou inconsciemment, par le désir des gouvernements de rendre la guerre inévitable? Les deux premières catégories font état de problèmes qui leur ont souvent été reprochés – évaluation des sources, partage des informations et rigidité intellectuelle – et qui ont inspiré de nombreux auteurs. La troisième, qui soulève la question des relations entre le milieu du renseignement et la classe politique et celle de l'utilisation publique des renseignements, est beaucoup plus récente. La récurrence des « vieilles » lacunes complique les projets de réforme, tandis que les « nouveaux » défis soulèvent un éventail de nouvelles interrogations.

Vieux reproches

Forts de l'échec du groupe d'inspecteurs de l'ISG, qui n'a trouvé aucune preuve de l'existence d'ADM en Irak, en dépit de ce qu'avaient affirmé les autorités américaines, britanniques et australiennes avant l'invasion de l'Irak, les opposants à la guerre ont accusé les gouvernements de la coalition d'avoir trompé les électeurs sur les raisons d'engager les hostilités. Dès le moment où les déclarations d'avant-guerre des gouvernements sur l'arsenal d'ADM de l'Irak et ses activités connexes étaient examinées de plus près, il était inévitable que les services de renseignement, sur les informations et les opinions desquels reposaient ces déclarations, soient entraînés dans la controverse. Au fil du débat, trois renseignements bien précis, qui avaient permis de conclure que les Irakiens étaient sur le point de fabriquer des ADM, ont plus particulièrement attiré l'attention. Selon certains rapports, l'Irak avait tenté de négocier l'achat d'uranium avec le Niger. D'autres affirmaient qu'il avait importé des aimants et d'importantes quantités de tubes en aluminium de

---

[7] Paul Robert, « Le Nouveau Petit Robert », p. 1265; (INFORM.) Qui procède par évaluations successives et hypothèses provisoires; qui sert à découverte.

grande résistance qui pouvaient servir à équiper des centrifugeuses au gaz pour l'enrichissement de l'uranium, et d'autres encore indiquaient que le régime de Saddam HUSSEIN avait fabriqué plusieurs laboratoires mobiles pour la fabrication d'armes biologiques. Chacun de ces renseignements a été utilisé par les autorités australiennes, britanniques et américaines dans des discours en faveur de la guerre, puis publiquement mis en doute peu de temps après le début du conflit. Le quotidien italien *La Repubblica* a publié des photos de documents visiblement faux dont était inspirée une partie au moins des rapports sur les efforts présumés de l'Irak pour acheter de l'uranium du Niger, et un ancien diplomate américain, Joseph WILSON, a rendu public les conclusions négatives de sa mission d'information officielle à ce sujet au Niger[8]. Selon des scientifiques qui ont témoigné auprès de l'Agence internationale de l'énergie atomique (AIEA) avant le déclenchement de la guerre, à moins de subir d'importantes modifications, les tubes d'aluminium ne pouvaient être d'aucune utilité dans une centrifugeuse pour l'enrichissement de l'uranium. Quant aux véhicules que l'on soupçonnait d'être des laboratoires mobiles d'armes biologiques, les inspecteurs de l'ISG ont constaté qu'ils devaient être utilisés à d'autres fins. À la fin de 2005, des représentants du Service fédéral allemand de renseignement extérieur ont révélé que la CIA avait été bien naïve d'accorder foi aux déclarations d'un transfuge irakien peu fiable dont le nom de code était « Curveball » sur les laboratoires mobiles d'armes biologiques[9].

Les enquêtes sur les renseignements menées aux États-Unis, au Royaume-Uni et en Australie après le début de la guerre ont toutes reproché aux organismes de collecte et d'analyse concernés de ne pas avoir minutieusement analysé les informations fournies par les sources humaines (HUMINT). En Australie, le comité parlementaire mixte de l'ASIO, de l'ASIS et de la DSD, le PJCAAD, a cité un témoin de l'enquête Hutton, au Royaume-Uni, selon qui les services qui obtiennent leurs renseignements de sources humaines ont tout intérêt à exagérer la fiabilité de celles-ci pour convaincre les destinataires des renseignements de leur importance et de leur utilité. Au Royaume-Uni, l'enquête Butler a constaté que l'urgence ressentie par les services de renseignement de clarifier la situation sur l'arsenal d'ADM de l'Irak et sa capacité de fabriquer de telles armes les a poussés à exercer davantage de pressions sur les sources humaines. Soit ils ont davantage accordé crédit à des sources non confirmées et accepté de se fier à des chaînes de renseignements dont la longueur aurait été jugée inacceptable en d'autres temps, soit ils les ont pressées de fournir des informations dans des domaines qui ne relevaient pas de leur champ de compétence habituel[10]. L'ASIS a échappé à la plupart des critiques qu'ont essuyées ses homologues américains et britanniques parce que près de 97 pour 100 des renseignements bruts sur lesquels les services australiens avaient fondé leur opinion provenaient de sources alliées. Dans le cas de l'Australie, le problème s'est posé différemment. Les renseignements humains reçus d'autres services doivent

---

[8] Les services secrets britanniques maintiennent que les informations sur les tractations présumées entre l'Irak et le Niger étaient fondées et provenaient d'une source humaine (HUMINT) sur laquelle ils ont toutefois refusé de fournir quelque précision que ce soit.

[9] Bob DROGIN et John GOETZ, « U.S. Whiffs on 'Curveball': Close Up », *The Los Angeles Times*, 27 novembre 2005.

[10] Lord BUTLER of Brockwell, KG, GCB, CVO, *Review of Intelligence on Weapons of Mass Destruction*, rapport d'un comité de conseillers, membres du Conseil privé, Chambre des communes, Londres, The Stationery Office, 2004, p. 108.

finalement être acceptés de confiance. Il faut tenir pour acquis que ces services ne communiquent que ce qu'ils jugent crédibles. La description des sources humaines doit évidemment demeurer vague, par souci de leur sécurité. Compte tenu de l'augmentation astronomique du nombre de rapports que les services de collecte ont dû rédiger, ces descriptions ont souvent été réduites à des formules toutes faites, choisies dans une « liste déroulante » d'une application informatique. Malgré tout, les organismes d'analyse australiens ont été accusés d'avoir manqué d'esprit critique dans l'évaluation de ces renseignements. L'ONA, en particulier, a été accusé, comme ses homologues américains et britanniques, d'avoir tiré des conclusions trop catégoriques des renseignements disponibles. Comme le PJCAAD l'a sévèrement constaté dans son rapport, « Toute décision de participer à une guerre et de risquer la vie d'un nombre élevé de gens ne doit reposer que sur les informations les plus sûres, des informations auxquelles les services australiens peuvent raisonnablement se fier »[11].

À mesure que l'onde de choc des attentats à la bombe de Bali s'est propagée au sein de la société australienne, un certain doute a commencé à se faire jour : cette opération terroriste était-elle, elle aussi, attribuable à une défaillance des services de renseignement, comme cela semblait être le cas dans le dossier des attentats du 11 septembre? L'attention s'est rapidement tournée vers le site Web du ministère des affaires étrangères et du commerce, le DFAT, où on pouvait lire au moment des attentats que le risque de violence en Indonésie était « élevé », mais aussi que « tout [fonctionnait] normalement dans les autres destinations touristiques ailleurs dans le pays, y compris à Bali ». Il est également apparu que les États-Unis avaient diffusé un avis aux voyageurs sur Bali à la fin de septembre 2002 et que leur ambassadeur à Canberra avait informé le gouvernement australien des risques d'attentats imminents à Bali la veille même des attentats[12]. Aux États-Unis, où se poursuivait l'autopsie des attentats du 11 septembre, il devenait de plus en plus évident que l'appareil américain du renseignement avait reçu des informations sur l'imminence d'attentats, mais que les divers services avaient omis soit de se communiquer ces informations, soit de prendre les mesures nécessaires après les avoir reçues. La commission d'enquête sur les attentats du 11 septembre a subséquemment utilisé le mot « vide » pour décrire l'absence de communication entre les services responsables des menaces extérieures et des menaces intérieures[13]. Dès lors, la tragédie de Bali aurait-elle pu être évitée elle aussi et ne s'est-elle produite qu'en raison de l'absence de communication entre les services australiens?

Une commission d'enquête parlementaire ayant conclu qu'aucun renseignement précis n'aurait pu permettre aux autorités de conclure à l'imminence d'un attentat à Bali en octobre 2002, le débat s'est

---

[11] Commonwealth of Australia, *Intelligence on Iraq's Weapons of Mass Destruction*, rapport du comité parlementaire mixte de l'ASIO, de l'ASIS et de la DSD, Canberra, CanPrint Communications, décembre 2003, p. 74 (appelé ci-après « rapport du PJCAAD »).

[12] *New York Times*, 20 octobre 2002.

[13] Philip ZELIKOW et al., *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, édition autorisée, New York, WW Norton and Company, 2004, p. 263.

concentré sur un autre aspect du problème : l'avis aux voyageurs du DFAT n'avait pas « bien reflété » les évaluations de renseignement sur les risques que les groupes islamistes radicaux faisaient peser sur les étrangers en Indonésie[14]. Dans leur témoignage au cours de l'enquête, le DFAT et l'ASIO avaient tous deux reconnu qu'ils ne s'étaient pas concertés sur la rédaction ou le contenu de l'avis aux voyageurs et qu'ils avaient travaillé « trop en vase clos ». Pourtant, ce problème précis mis à part, les membres de l'AAR étaient convaincus qu'une telle négligence et qu'un tel manque de communication ne se produiraient jamais en Australie, puisqu'il est clair depuis longtemps que l'ASIO est le principal service de la lutte contre le terrorisme. La loi le constituant établit clairement que son domaine de responsabilité ne concerne pas uniquement le renseignement intérieur, mais aussi le renseignement de sécurité, c'est-à-dire les menaces intérieures et extérieures. De fait, outre ses responsabilités en matière de collecte de renseignements sur les menaces intérieures, l'ASIO a toujours eu accès à tout renseignement utile sur l'étranger recueilli par l'AAR.

Il ne faut toutefois pas conclure que l'AAR ferme les yeux sur ces problèmes de communication potentiels. À l'ère des menaces transnationales, la multiplication des services gouvernementaux qui interviennent dans le processus du renseignement exige de bonnes communications avec les acteurs peu familiarisés avec les pratiques et le rôle de l'AAR. L'appareil du renseignement élargi doit assurer le maintien de la sécurité et la connectivité des systèmes d'information et, surtout, prendre en compte les différences culturelles en matière d'information. Les organisations ne définissent en effet pas toutes de la même manière ce qui constitue un renseignement important ou une information documentaire, ce qui peut et doit être partagé et ce qui ne le doit pas. Le défi le plus important réside peut-être dans l'établissement de communications efficaces et harmonieuses avec l'AFP, la police fédérale australienne, dont les opérations à l'étranger permettent de recueillir une foule de renseignements précieux sur les menaces transnationales. Le travail de renseignement est essentiellement prospectif, puisqu'il s'agit d'essayer de prévoir et de contrer les nouvelles menaces pour l'État et la société. Par comparaison, le travail de police a habituellement pour but de recueillir de nouvelles preuves chaque fois qu'un crime a été commis. Comme l'a déclaré un témoin au cours de l'enquête sur les attentats du 11 septembre, les services de collecte de renseignements sur l'étranger ont tendance à adopter une attitude défensive et à se tenir à l'affût des tendances et de l'évolution de la situation dans les secteurs géographiques qui relèvent de leur responsabilité, tandis que les services de l'ordre se battent « à un contre un », cherchant les coupables de délits et les traquant une fois qu'elle a établi leur identité[15]. Au chapitre du partage de l'information, les difficultés abondent. Les services de renseignement ne permettent pas que des informations secrètes soient utilisées pour constituer une preuve criminelle contre les auteurs de délits transnationaux, tandis que les corps policiers refusent que des éléments de preuve déterminants dans une enquête en cours soient communiqués à quiconque ne participe pas à cette enquête. Il arrive ainsi fréquemment

---

[14] Commonwealth of Australia, *Bali 2002: Security Threats to Australians in Southeast Asia*, rapport du comité mixte du Sénat des affaires étrangères, de la défense et du commerce, Canberra, Senate Printing Unit, août 2004 (appelé ci-après « Rapport du JFADT »), p. xvii.

[15] Rapport de la commission d'enquête sur les attentats du 11 septembre, p. 268.

que les uns ne se rendent pas compte qu'ils possèdent des informations qui seraient utiles aux autres.

Les services de renseignement australiens, tout comme leurs homologues américains et britanniques, ont aussi été accusés d'avoir manqué d'esprit critique dans leur analyse des capacités de l'Irak en matière d'ADM. Comme ils ne disposaient que d'informations vagues et incomplètes sur ses activités dans ce domaine, les services d'évaluation ont déduit du comportement passé des Irakiens en matière d'acquisition d'armes et de leurs efforts continus pour se soustraire au processus d'inspection qu'ils possédaient de telles armes et qu'ils cherchaient à les cacher. Cette opinion a été examinée à la loupe quand les équipes d'inspection de l'ISG ont déclaré, après le déclenchement de la guerre, qu'il n'y avait pas d'ADM en Irak. Selon le rapport Flood, les services australiens « ont manqué de rigueur en ne contestant pas les idées reçues ou les hypothèses sur les intentions du régime irakien » et, de façon plus générale, « qu'il n'existe au sein des services de collecte de renseignements pour ainsi dire aucune culture de contestation et de discussion systématiques des rapports de renseignements, sans parler de l'absence quasi totale de dialogue sur les informations évaluées »[16]. Comme les explications basées sur la « pensée de groupe » ou la « dissonance cognitive » dominent dans nombre d'études savantes sur les défaillances du renseignement[17], les commentateurs ont aussi mis l'accent sur l'étroitesse d'esprit et le manque de rigueur intellectuel de l'AAR[18]. Éclairés par la compréhension a posteriori des événements, les responsables des diverses commissions d'enquête ont proposé d'autres pistes pour expliquer les efforts de Saddam HUSSEIN pour cacher ses ADM. Elles vont du bluff et de la fierté nationale[19], à la stratégie de la corde raide et aux erreurs de calculs[20], en passant par la paranoïa et le contexte politique chaotique de la dictature[21]. L'analyse du renseignement, comme toute autre activité dans laquelle intervient l'interprétation, est sujette à ce que Robert JERVIS appelle le « chauvinisme de l'expert », c'est-à-dire qu'une longue expérience et qu'une connaissance approfondie d'un sujet apportent une certitude supplémentaire et un certain degré d'incontestabilité aux opinions émises[22]. Dans le cas de l'Irak et de ses manoeuvres pour cacher ses ADM, l'évaluation initiale a mis en branle un processus circulaire de collecte et d'analyse qui a été alimenté, à partir de la fin de 2002, par un nombre sans

---

[16] Rapport Flood, pp. 25 et 26.

[17] Par exemple, Irving L. JANIS, *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes*, Boston, Houghton Mifflin, 1972; Roberta WOHLSTETTER, *Pearl Harbor: Warning and Decision*, Stanford, Stanford University Press, 1962.

[18] Paul MONK, « Why Didn't We Think of That? », *Australian Financial Review*, 2 novembre 2001; Lee CORDNER, « Reaping the Rewards: Executive Expectations of the Intelligence Investment », *Future Directions International*, mai 2003, p. 3.

[19] Rapport du PJCAAD, p. 80.

[20] Rapport Flood, p. 23.

[21] Rapport Butler, p. 15.

[22] Robert JERVIS, « What's Wrong with the Intelligence Process? », *International Journal of Intelligence and Counter-Intelligence*, vol. 1, 1986, pp. 31 et 32.

cesse croissant de renseignements sur les efforts des Irakiens pour cacher leurs armes, ce qui a contribué à renforcer l'opinion qu'en agissant ainsi, ceux-ci en confirmaient l'existence[23]. Ce qui met en lumière un danger connexe : comme les analystes doivent consacrer de plus en plus de temps à l'assimilation d'un nombre sans cesse croissant de renseignements, ils peuvent être tentés de penser que les tendances inférées à partir des renseignements secrets représentent la réalité quand, dans les faits, ils n'en donnent qu'une image instantanée, fournie par les sources que les services de collecte sont en mesure de côtoyer et de recruter. Enfin, il existe un risque connexe de « fétichisation » du renseignement secret, c'est-à-dire de le considérer plus précieux et plus révélateur, en soi, que tout autre type d'information[24].

Le dernier reproche souvent adressé à l'AAR concerne l'étroitesse de ses relations avec les services secrets américains et britanniques, relations qui l'auraient amené à se comporter en marionnette crédule et à entraîner (une fois de plus) l'Australie dans des « guerres qui ne la regardent pas »[25]. L'alliance UKUSA, qui regroupe les États-Unis, le Royaume-Uni, le Canada, l'Australie et (autrefois) la Nouvelle-Zélande et établit entre eux un étroit réseau d'échange de renseignements, est dénoncée depuis longtemps, ses détracteurs affirmant qu'elle constitue un important outil de « colonisation » de la pensée stratégique de l'Australie par ses puissants alliés[26]. Selon un observateur, des « exagérations et des erreurs similaires » ont été relevées dans les arguments en faveur de la guerre avancés par les Australiens, les Américains et les Britanniques, ce qui donne largement à entendre que l'AAR s'est contenté de répondre aux demandes du gouvernement en régurgitant « des renseignements qui avaient d'abord été assimilés par les Américains et les Britanniques »[27]. Prenant ces accusations au sérieux, le comité parlementaire d'enquête sur les ADM irakiennes s'est penché sur ce qu'il a appelé l'« indépendance extérieure de l'AAR – les évaluations sont fonction de l'intérêt national de l'Australie et non de celui d'autres nations[28]. En raison de la spécialisation géographique des partenaires de l'alliance UKUSA et de la taille moins imposante de l'AAR, 97 pour 100 des renseignements bruts sur les ADM de l'Irak environ ont été recueillis par les services américains et britanniques. Comme l'a souligné le rapport Flood, « les analystes peuvent difficilement demander des précisions sur les renseignements fournis par les services étrangers et les mettre en doute... en général, les descriptions des sources ne leur étaient d'aucune utilité et

---

[23] Rapport Butler, p. 89.

[24] WESLEY, « Analysing Transnational Intelligence », p. 102.

[25] Peter MANNING, « A Colonial State of Mind », *Griffith Review*, n° 5, printemps 2004.

[26] Voir, par exemple, Joseph A. CAMILLERI, *ANZUS : Australia's Predicament in the Nuclear Age*, Melbourne, Macmillan, 1987.

[27] Geoffrey BARKER, *Sexing It Up: Iraq, Intelligence and Australia*, Sydney, UNSW Press, 2003, p. 79.

[28] Rapport du PJCAAD, p. 44.

semblaient tirées d'une liste réduite de phrases toutes faites »[29]. Les services australiens se sont également tenus au courant des opinions des Américains et des Britanniques sur les ADM irakiennes et les liens avec AL-QAÏDA. Ces constatations ne permettent toutefois pas nécessairement de conclure que les évaluations des services australiens n'étaient qu'une copie conforme de celles de leurs homologues américains et britanniques. Le comité parlementaire et la commission d'enquête Flood ont tous deux conclu que les services australiens avaient fait preuve de « beaucoup plus de retenue » sur la question des capacités de l'Irak en matière d'ADM que leurs homologues à Washington et à Londres. Ils ont par exemple rejeté les déclarations des Américains sur les liens de Saddam HUSSEIN avec AL-QAÏDA et les affirmations des Britanniques sur la capacité de l'Irak de déployer des ADM en 45 minutes. De telles divergences d'opinion, certes mineures mais néanmoins éloquentes, entre les alliés donnent à penser que l'AAR a pris au sérieux la responsabilité qui lui incombe d'évaluer avec un esprit critique les renseignements bruts qu'il reçoit et de se faire sa propre opinion. Enfin, le scandale qui a éclaté au milieu de 2003 quand les services australiens ont été accusés d'avoir négligé d'informer le gouvernement des doutes du bureau américain de renseignement et de recherche, l'INR, sur les rapports de renseignements sur les tentatives des Irakiens de se procurer de l'uranium en Afrique a montré qu'ils n'étaient pas de simples « courroies de transmission » des évaluations américaines et britanniques[30].

Nouveaux reproches

Le comité parlementaire mixte d'enquête sur les renseignements sur les ADM irakiennes a constaté que l'opinion de l'ONA sur les armes irakiennes a changé presque du jour au lendemain au milieu de septembre 2002 quand il a commencé à « utiliser l'indicatif plutôt que le subjonctif dans ses déclarations [sur les capacités des Irakiens en matière d'ADM], accroissant ainsi le degré de culpabilité de l'Irak et le degré de certitude des analystes »[31]. Il aurait adopté ce ton plus catégorique dans ses évaluations, a-t-on laissé entendre, en réponse à une demande du cabinet du ministre des affaires étrangères, Alexander DOWNER, qui souhaitait obtenir toutes les informations non classifiées disponibles sur les activités de l'Irak dans le domaine des ADM. Il s'est ensuivi un déluge d'accusations de « politicisation » de l'AAR. Dans le rapport Flood, ce mot s'applique autant au contenu des rapports qu'à ce qui n'y figure pas. Dans le premier cas, le risque réside dans le fait que le gouvernement ou les services des politiques exercent ouvertement des pressions en faveur d'une opinion donnée ou dans le fait que l'analyste cherche inconsciemment à favoriser un résultat donné. Dans le deuxième cas, les analystes et les administrateurs peuvent choisir, consciemment ou non, de ne pas rédiger de rapport sur une question précise qui pourrait mettre le gouvernement dans

---

[29] Rapport FLOOD, p. 25.

[30] « Australian Intelligence Agency Admits It Did Not Tell Government of US Doubts Over Iraqi Evidence », Associated Press, 10 juillet 2003; « The PM and the Public Service », *Sydney Morning Herald*, 15 juillet 2003; Allan BEHM, « How We Got Iraq's WMDs Wrong », *The Australian*, 14 juillet 2003.

[31] Rapport PJCAAD, p. 33.

l'embarras[32].

De l'avis des commentateurs, la politicisation de l'AAR date du jour où les directeurs des services de renseignement ont été invités à participer aux voyages du premier ministre[33] et aux réunions du comité du Cabinet chargé de la sécurité nationale[34], ou du jour où des carriéristes, doublés de « fins politiques », issus des services des politiques[35], qui croient qu'ils « compromettent leurs chances d'avancement s'ils donnent aux ministres des conseils difficiles à accepter ou leur communiquent des informations qu'ils ne voulaient pas entendre » ont été nommés aux postes de direction de l'AAR[36]. D'autres affirment que l'ONA a repoussé son souci de l'intérêt politique au second plan, au profit de la défense d'intérêts politiques, c'est-à-dire qu'il opère une sélection parmi les renseignements, ou les module, pour donner l'illusion qu'une certaine politique donne les résultats escomptés ou est adaptée aux besoins, en dépit des preuves du contraire[37]. Certains commentateurs ont accusé l'AAR de ne pas intervenir suffisamment dans le processus politique, sous-entendant ainsi que les évaluations de renseignements servent « à contester et à remettre en question la sagesse conventionnelle des ministères [et] à s'y opposer »[38] ou soutenant qu'il « n'était pas parvenu... à amener les décideurs à apprendre »[39] ou encore que « les responsables du renseignement ont échoué » si le décideur, dans ce cas-ci le chef du gouvernement, rejette des renseignements vitaux et n'y donne pas suite[40].

La confusion des rôles entre le monde du renseignement et la sphère politique touche à l'essence même du principe organisationnel fondamental de l'AAR. En 1977, le rapport Hope a recommandé la création de l'ONA ainsi que l'officialisation des mécanismes de coordination et de surveillance de l'AAR, reprenant à son compte le conseil de Walter Lippmann : « La seule garantie institutionnelle [de l'objectivité et de l'impartialité de l'analyse] réside dans la séparation la plus

---

[32] Rapport Flood, p. 105.

[33] Tom ALLARD, « The War of Secrets », *Sydney Morning Herald*, 6 mars 2004.

[34] Allan GYNGELL, « Closer Ties That Weaken the System », *Sydney Morning Herald*, 24 février 2004.

[35] Andrew WILKIE, « A Lack of Intelligence », *Sydney Morning Herald*, 31 mai 2003.

[36] BARKER, *Sexing It Up*, p. 73; voir aussi Philip KNIGHTLY, « Deadly Secrets », *The Bulletin*, 122, 27 avril 2004; Tom ALLARD, « Canberra Was Warned on Spy Reports, Says Ex-Analyst », *Sydney Morning Herald*, 27 mai 2003.

[37] « ONA's Independence is Part of a Delicate Balance », *Sydney Morning Herald*, 15 avril 2004.

[38] Gary KLINTWORTH, « Flood Report: Mild Applause », *Asia Pacific Defence Reporter*, septembre 2004, p. 12.

[39] Paul MONK, « Learning to See », *Griffith Review*, n° 5, printemps 2004.

[40] CORDNER, « Reaping the Rewards », p. 3.

complète possible entre le pouvoir exécutif et les responsables des enquêtes. Ils doivent évoluer dans deux univers parallèles mais parfaitement étanches, sans accorder aucun intérêt à leurs succès respectifs ». Pour le non-initié, le glissement du processus d'analyse du renseignement, dont l'objet est de rédiger des rapports utiles mais objectifs à l'intention des politiques, vers la rédaction de rapports qui devraient plaire aux ministres et soutenir leurs politiques semble aller de soi, à première vue, voire même être inévitable. Si le principe d'utilité conduit à la marginalisation, il peut effectivement devenir difficile « de ne pas céder à l'envie de dire aux décideurs ce qu'ils veulent entendre »[41]. Il faut toutefois se garder de sauter trop rapidement à de telles conclusions. Les gouvernements démocratiques ont, par définition, horreur du risque. Comme toute erreur d'ordre politique ou toute décision confirmée de ne pas prendre des indices d'un danger imminent au sérieux risque de leur coûter cher politiquement parlant, les autorités sont prêtes à assumer des coûts beaucoup plus élevés à court terme pour atténuer tout risque potentiel à long terme. Les services de renseignement ont précisément pour mandat de prévenir les gouvernements des risques émergents. Comme, de nos jours, les médias et les parlementaires scrutent les décisions prises par les gouvernements et les informations dont ils disposaient à la loupe, les services et les agents de renseignement courent davantage de risques en n'informant pas les autorités de dangers graves ou en ne leur fournissant pas des preuves tangibles de l'inefficacité de leurs politiques qu'en leur disant ce qu'elles ne veulent pas entendre. Aucun directeur de service de renseignement ne resterait longtemps en poste s'il s'avérait qu'il a caché, ignoré ou rejeté sans aucun motif valable un élément d'information susceptible de compromettre sérieusement le succès de la politique gouvernementale. Si l'important, pour les responsables du renseignement, c'est de capter l'attention des ministres, ils y parviendront plus sûrement en leur communiquant des informations désagréables ou des mises en garde bien étayées qu'en ne leur soumettant que des preuves de la sagesse ou de l'efficacité d'une politique. En outre, un gouvernement qui laisse délibérément ou tacitement le rôle de ses services de renseignement glisser vers la défense des politiques risque de se priver d'un mécanisme qui a précisément été mis en place pour l'informer de l'imminence d'un danger ou de l'inefficacité de ses politiques. Les services de renseignement doivent demeurer soucieux de l'intérêt politique, c'est-à-dire comprendre quels dossiers revêtent de l'importance aux yeux du gouvernement, à quel moment des informations supplémentaires contribueront à la prise de décisions et comment les renseignements sont utilisés pour orienter les décisions et la politique. Ils devraient donc avoir pour rôle de renseigner le gouvernement sur la sagesse, la pérennité et l'efficacité des politiques à partir des informations disponibles. Dans un tel contexte, les accusations de politicisation de l'AAR demeurent graves, mais son manque apparent de jugement sur la question des ADM irakiennes ne constitue pas une preuve suffisante. Bien que les critiques aient rejeté le rapport Flood en déclarant qu'il ne fallait pas s'attendre à autre chose de la part d'un « initié », son auteur a conclu, avec raison, qu'il n'existait aucune preuve de la politicisation de l'AAR.

Un autre sujet connexe, à savoir l'utilisation publique de renseignements par les autorités, a lui aussi soulevé la controverse. Le gouvernement australien a, à cet égard, devancé Washington et Londres lorsque le premier ministre, John Howard, a clairement cité un rapport de l'ONA à l'appui de la

---

[41] Desmond BALL, « Silent Witness: Australian Intelligence and East Timor », *The Pacific Review*, vol. 14, n° 1, 2001, p. 36.

position de son gouvernement dans le dossier des demandeurs d'asile juste avant l'élection fédérale de novembre 2001. Puis, dans les mois qui ont précédé le début du conflit en Irak, le gouvernement australien a multiplié les allusions aux renseignements qu'il possédait dans son plaidoyer en faveur de la guerre, n'allant toutefois pas, contrairement à ses homologues américain et britannique, jusqu'à les citer dans ses déclarations publiques. Au milieu du mois de septembre 2002, le cabinet du ministre des Affaires étrangères, Alexander DOWNER, a demandé un document non classifié faisant état de tous les renseignements selon lesquels l'Irak possédait des ADM. Comme l'ont souligné les membres de la commission Butler au Royaume-Uni, ces procédés, c'est-à-dire l'utilisation directe de renseignements à l'appui d'une politique et la rédaction sur demande par les services de renseignement de documents destinés à être rendus publics ou à servir de canevas aux déclarations d'un ministre, étaient sans précédent[42]. En Australie, une telle utilisation des renseignements a donné lieu à deux critiques majeures. Il a tout d'abord été reproché aux autorités de s'être servies de l'autorité et de l'objectivité de l'AAR à mauvais escient, pour consolider leur position. Un aspect, surtout, a retenu l'attention. Le gouvernement avait affirmé que les services de renseignement avaient « avalisé » les déclarations ministérielles en faveur de la guerre. Lorsque les travaux du PJCAAD ont révélé que l'ONA avait uniquement vérifié l'exactitude des extraits qui avaient été tirés des renseignements fournis, le comité a très mal réagi au raisonnement casuistique du gouvernement.

L'obligation d'exactitude vaut aussi pour l'ensemble de la situation décrite. Passer certaines opinions ou certains faits importants sous silence dans la citation d'une évaluation de renseignements peut entraîner une déformation des faits. Toute interprétation exacte et fidèle de celle-ci doit reposer sur l'ensemble du point de vue invoqué à l'appui d'une politique[43].

En agissant ainsi, le gouvernement court le risque de miner « la confiance du public dans l'utilité et la fiabilité des renseignements »[44]. En outre, en ayant été contraint de troquer son rôle de rédacteur de rapports de renseignements pour celui de fournisseur d'informations grand public, l'AAR avait-il sacrifié l'exactitude au profit de la cohérence et de la facilité de compréhension? Tout écrit destiné au grand public, a-t-on donné à entendre, met nécessairement l'accent sur les avis exprimés plutôt que sur les détails et les failles des preuves. Voilà ce que le PJCAAD a suggéré dans son rapport en datant – sans fournir de preuve de l'existence d'un lien de causalité –, l'atténuation par l'ONA des doutes et des failles dans les renseignements sur la présence d'ADM en Irak du moment où il a rédigé un rapport de renseignement non classifié à l'intention du cabinet du ministre des Affaires étrangères. Cette utilisation publique des renseignements a donné naissance aux accusations de politicisation de l'AAR.

---

[42] Rapport Butler, p. 76.

[43] Rapport du PJCAAD, pp. 93 et 94.

[44] *Ibid.*, p. 74.

La tentation qu'éprouvent les gouvernements d'utiliser les renseignements au grand jour ne disparaîtra sans doute pas. Dans le cas des menaces transnationales qui, de par leur nature même, émergent sans que l'on s'y attende, les nouveaux impératifs de sécurité exigent que l'impossible soit mis en oeuvre pour qu'elles ne se matérialisent pas. Comme l'a déclaré le premier ministre de Grande-Bretagne, Tony BLAIR, au président des États-Unis, George W. BUSH, lors d'une rencontre à Crawford (Texas) en avril 2002, laisser, par inertie ou insouciance, ces menaces prendre de l'ampleur « serait ignorer les leçons du 11 septembre »[45]. Par contre, en démocratie, il faut fournir à la population une explication logique des motifs à l'origine d'une politique, même s'ils ne sont pas évidents. Il est dès lors difficile de renoncer à utiliser les renseignements disponibles pour appuyer un discours en faveur d'une intervention. Comme M. BLAIR l'a indiqué à la commission Butler, « la diffusion [au grand public de renseignements fournis par les services britanniques] avait tout simplement pour but de dire "Voilà pourquoi nous pensons que c'est important ... Voilà les renseignements qui prouvent qu'il ne s'agit pas du fruit de notre imagination, le problème est bien réel "»[46]. Il existe une distinction subtile entre fournir à la population et à l'opposition un même ensemble de renseignements objectifs à partir duquel elles pourront juger de la sagesse des politiques proposées et utiliser ces mêmes renseignements pour soutenir une politique gouvernementale. En Australie, le contre-ministre des Affaires étrangères, Kevin RUDD, a accusé le gouvernement d'avoir succombé à la tentation en ne « choisissant » dans les rapports que les renseignements qui appuyaient son plaidoyer en faveur de la guerre[47]. En agissant ainsi, les gouvernements courent le risque de diminuer graduellement la fiabilité des renseignements et de ne plus pouvoir les invoquer pour expliquer les mesures politiques prises contre les menaces transnationales si l'opinion publique a le sentiment qu'ils les utilisent à mauvais escient ou à des fins partisanes, ou encore s'ils s'avèrent que ceux-ci sont faux.

3. Les réformes

Les pressions nées des lacunes récurrentes de l'AAR ont contribué à en accroître l'efficacité, mais dans ce cas-ci, c'est sa probité qui est mise en cause. Les récentes réformes inspirées de ces nouveaux problèmes ont porté sur trois grands aspects de ses activités : renforcement des principes structurants et refonte des mécanismes de coordination, amélioration de la surveillance exercée par des organismes de l'extérieur et augmentation des ressources et de la taille de la plupart des services de renseignement.

Différenciation fonctionnelle et coordination

Devant les preuves des lacunes « horizontales » des services de renseignement – vérification

---

[45] Rapport Butler, p. 71.

[46] Rapport Butler, p. 77.

[47] Cynthia BANHAM, « Report is Proof of Deception », *Sydney Morning Herald*, 2 mars 2004.

défaillante des sources, « compartimentation » des renseignements et « cloisonnement » des rôles d'alerte, acceptation des opinions sans les contester –, certains commentateurs ont suggéré d'imiter les Américains et de fusionner l'AAR et les services d'application de la loi en un nouveau ministère de la sécurité nationale. Un parti d'opposition, le Parti travailliste, en a fait son cheval de bataille. Le rapport Flood et le gouvernement ont cependant rejeté l'idée d'une restructuration aussi radicale, choisissant plutôt de réitérer la distinction fonctionnelle dans les domaines où elle n'était plus aussi claire et de renforcer les mécanismes de coordination de l'AAR[48]. Dans son rapport, M. FLOOD a souligné que « la distinction bien nette des rôles de chaque membre de l'appareil australien du renseignement et l'absence presque complète de chevauchement des compétences constituent l'un des points forts du système australien[49]. On n'y observe pas non plus les problèmes de partage des renseignements constatés aux États-Unis[50] ou au Royaume-Uni[51], en partie parce que chaque service est spécialisé et qu'il sait qu'il dépend des autres. Les membres de l'AAR sont fermement convaincus que les différents aspects du travail de renseignement requièrent des cultures organisationnelles différentes. Le principe de la distinction fonctionnelle a été clairement réaffirmé lorsque les rôles respectifs des deux services d'évaluation, l'ONA et la DIO, ont été redéfinis. Le domaine de compétence de la DIO a été rigoureusement circonscrit à l'analyse des renseignements destinés au ministère de la Défense et aux forces armées australiennes, tandis que l'ONA a été « reconfirmé » dans son rôle de « principal organisme national d'évaluation du renseignement sur l'étranger ». M. FLOOD et le gouvernement ont rejeté les critiques selon lesquelles cette différenciation des rôles privait l'AAR d'une source de contestation des renseignements, dont il a pourtant bien besoin, faisant plutôt valoir qu'ils faisaient une meilleure utilisation des ressources en encourageant le débat et la contestation au sein même de l'ONA et de la DIO.

Une fois réitéré le principe de la distinction fonctionnelle, il fallait améliorer la coordination du renseignement. Des mécanismes ont été ajoutés, à cette fin, à tous les niveaux. L'Australie a suivi l'exemple des États-Unis et du Royaume-Uni et créé un centre mixte et polyvalent d'évaluation de la menace terroriste ouvert 24 heures sur 24, le National Threat Analysis Centre (NTAC). Son personnel, qui est logé dans les locaux de l'ASIO, se compose d'employés détachés par chacun des services membres de l'AAR ainsi que l'AFP, le MAEC et le ministère des transports et des services ruraux. Il est reconnu comme la seule source autorisée d'avis sur la menace et participe régulièrement à la rédaction des avis aux voyageurs du MAEC. Les réformes effectuées dans la foulée du rapport Flood ont entraîné la création d'un comité de coordination du renseignement sur l'étranger, le FICC, l'augmentation des ressources de l'ONA et le renforcement du rôle de coordinateur de l'AAR qui lui incombe ainsi qu'à son directeur général. Le FICC a officialisé un

---

[48] Verona BURGESS, « Ruddock Rejects Mergers », *Australian Financial Review*, 11 mai 2005.

[49] Rapport Flood, p. 69.

[50] Rapport de la commission sur le 11 septembre, p. 353.

[51] Rapport Butler, p. 111.

comité des directeurs des services de renseignement qui existait officieusement, le HIAM. Tous les mois, ses membres, des représentants de l'AFP et des hauts fonctionnaires du MAEC, du bureau du premier ministre et du Cabinet (BPMC) tiennent une réunion de coordination. Présidé par le directeur général et appuyé par un secrétariat de l'ONA, le FICC s'occupe de la coordination, de la planification stratégique et de l'évaluation au sein de l'AAR. Il a la possibilité d'intervenir officiellement dans le processus politique par l'intermédiaire d'un nouveau service du BPMC, la division de la sécurité nationale, et du comité de la sécurité nationale des secrétaires, le SCONS, du comité national de la sécurité du Cabinet, le NSCC. Tous ces mécanismes ont été mis en place pour rendre l'ensemble du gouvernement plus attentif aux renseignements et qu'il en tienne davantage compte dans l'élaboration des politiques.

Le gouvernement australien a pu adopter une solution aussi simple au problème de la coordination horizontale en raison de la taille réduite de l'AAR et de sa culture déjà axée sur la collégialité. Les nouveaux mécanismes officiels de coordination s'inscrivent dans un cadre où les rôles et les responsabilités sont bien compris depuis longtemps. La nomination, au sein de l'AAR, de gestionnaires issus du MAEC et du ministère de la Défense, si souvent décriée parce qu'elle constitue « un nivellement par le bas » et en atténuait le professionnalisme, a permis d'implanter une culture pragmatique de coopération parmi les hauts dirigeants des services de renseignement. Cet engagement aux échelons les plus élevés favorise la coopération aux échelons les plus bas, ce qui garantit une approche beaucoup plus rigoureuse et judicieuse de la collecte du renseignement et de la rétroaction, le tout dans un esprit de plus grande collaboration. Il permet aussi de calmer les inquiétudes des services de collecte qui craignent qu'un processus de coordination et de surveillance trop rigoureux soit trop envahissant. Le rôle « discret d'agent lubrifiant » de la coopération au sein de l'AAR est si important que plusieurs craignent que la croissance et la professionnalisation qui résulteront des réformes préconisées par M. FLOOD en menacent la culture de collégialité tranquille.

Surveillance de l'extérieur

Au fil des ans, une série de scandales mettant en cause les services australiens de collecte de renseignements a donné lieu à un renforcement répété des mécanismes de surveillance de l'extérieur. Les principales innovations ont été la création d'un comité parlementaire mixte de l'ASIO, de l'ASIS et de la DSD et du poste d'inspecteur général du renseignement et de la sécurité, l'IGIS. Le titulaire de cette fonction, prévue dans la loi, est chargé de faire enquête sur les opérations et la probité des services de collecte de renseignements et de faire régulièrement rapport de ses constatations. Il peut en outre décider d'enquêter sur ces services et il est investi des pouvoirs d'une commission d'enquête parlementaire. Le PJCAAD et l'IGIS ont tous deux joué un rôle de premier plan, ces dernières années, dans l'évaluation de l'intégrité et de la compétence des services qui composent l'AAR.

Le rapport Flood a pris les accusations de politicisation de l'AAR au sérieux. Il a conclu que les services de renseignement australiens ne sont pas politisés, mais a néanmoins reconnu la nécessité de protéger leur réputation de rigueur et d'objectivité : « le fonctionnement des services de

renseignement australiens intéresse beaucoup le public et est surveillé de près ». Même s'il a reconnu que les services d'analyse des renseignements sur l'étranger menacent rarement les droits ou la vie privée des citoyens australiens, M. FLOOD a fait valoir que l'extension du pouvoir de surveillance du comité parlementaire à l'ONA et à la DIO « rassurerait le Parlement et la population en soumettant l'ensemble des services de renseignement à l'obligation de rendre des comptes à un groupe de parlementaires de haut rang ». Il a donc recommandé que le comité chargé de cette responsabilité adopte le nom de comité parlementaire mixte du renseignement et de la sécurité, PJCIS. Dans le même ordre d'idées, le rapport Flood a recommandé que les pouvoirs de l'IGIS visent aussi l'ONA et la DIO, qu'il soit habilité à mener des enquêtes, à sa discrétion, sur les activités des services d'analyse et, en particulier, qu'il se penche périodiquement sur l'indépendance, prévue par la loi, de l'ONA.

Les intentions qui ont inspiré ces réformes sont certes louables, mais elles pourraient difficilement se concrétiser sans compromettre la capacité des organismes d'analyse de donner des opinions rigoureuses et objectives. M. FLOOD semble reconnaître qu'il est risqué de soumettre les opinions des organismes d'analyse à l'examen régulier des parlementaires lorsqu'il suggère écrit ce qui suit : [Tout] comme les conseils des fonctionnaires aux ministres ne sont pas révélés devant le comité de la législation du Sénat, les opinions des services d'évaluation ne devraient pas être soumises à l'examen des parlementaires ». Il laisse plutôt entendre qu'outre les « questions d'ordre budgétaire et administratif » concernant l'ONA et de la DIO, « le processus dans le cadre duquel [ces deux organismes] produisent leurs évaluations pourrait également être soumis à l'examen des parlementaires »[52]. On imagine difficilement qu'un comité parlementaire se limiterait à ces questions. Comme le montre les travaux du comité du budget du Sénat, ceux-ci débordent régulièrement le cadre du simple examen « des questions d'ordre budgétaire et administratif ». Il sera en outre impossible d'examiner correctement le processus de production des évaluations sans avoir une idée de ce qu'elles contiennent. Qui plus est, la capacité des comités parlementaires d'agir comme organismes de surveillance impartiaux soulève de plus en plus de doutes, de nombreux commentateurs soulignant les clivages partisans de plus en plus tranchés qui caractérisent les débats sur la sécurité et le renseignement[53]. Les divergences dans les conclusions des deux commissions d'enquête sur les ADM irakiennes illustrent la subjectivité inhérente à tout examen des processus d'évaluation et de leurs résultats : selon le PJCAAD, l'ONA a durci ses positions à partir du milieu du mois de septembre 2002[54], tandis que d'après le rapport Flood, ces changements ne sont survenus qu'au début de 2003[55]. Comme les luttes partisanes et la subjectivité risquent d'entacher le

---

[52] Rapport Flood, p. 58.

[53] Voir, par exemple, Carl UNGERER, « Issues in Australian Foreign Policy: January to June 2004 », *Australian Journal of Politics and History*, vol. 50, n° 4, 2004.

[54] Rapport du PJCAAD, p. 33.

[55] Rapport du Report, p. 29.

processus d'examen parlementaire, il est difficile de croire que les services d'évaluation des renseignements ne tiendront pas compte de la possibilité que leurs opinions soient soumises à un tel examen quand ils les formuleront. Le danger réside dans le fait qu'ils pourront être tentés de se montrer plus prudents et de mesurer leurs propos, un comportement que de nombreux critiques ont justement attribué à la politisation de ces services et que les réformes sont censées éviter.

Ressources et expansion

Au fil des ans, les organismes qui composent l'appareil australien du renseignement et de la sécurité en sont venus à favoriser la qualité de leurs services plutôt que de chercher à multiplier ceux-ci. Ainsi, par comparaison aux autres organisations militaires régionales, la force de défense australienne est peu importante, mais s'enorgueillit du haut niveau d'entraînement de ses membres et de ses technologies avancées. De même, l'appareil du renseignement est demeuré beaucoup plus petit que celui des plus proches alliés de l'Australie. Les États-Unis consacrent cent fois plus de ressources que l'Australie au renseignement et la Grande-Bretagne, quatre fois plus. L'AAR a pu s'offrir ce luxe en partie parce qu'il sait qu'il appartient au plus puissant réseau de collecte de renseignements au monde, l'alliance UKUSA. Les cibles des activités de collecte des services australiens sont décrites on ne peut plus clairement dans le rapport Flood : « En ce qui concerne le sud-est asiatique et le sud du Pacifique, l'Australie doit jouer un rôle de chef de file dans le domaine du renseignement... Dans le cas du nord de l'Asie, elle doit être exceptionnellement bonne... Pour ce qui est du sud de l'Asie, elle doit être très bonne... »[56]. Ce qui laisse entendre que dans le cas des autres régions, elle peut s'en remettre à ses partenaires de l'alliance. En ce qui a trait à l'analyse, M. FLOOD a affirmé que « l'Australie doit conserver son indépendance sur toutes les questions sur lesquelles le gouvernement veut être conseillé. Elle doit être en mesure d'évaluer les renseignements obtenus d'autres sources d'un oeil critique[57].

Contraint, par des impératifs d'ordre politique, de ne négliger aucun effort pour protéger l'Australie contre les menaces transnationales, le gouvernement a commencé en 2001 à accroître les budgets et les pouvoirs des services de collecte de première ligne. Les dépenses en matière de renseignement étranger et de sécurité sont passées de 332 millions de dollars en 2000-2001 à 659 millions de dollars en 2004-2005 et ce, avant même l'adoption des réformes préconisées dans le rapport Flood. La très grande partie de cette augmentation a bénéficié à l'ASIO, à l'ASIS et au DSD. L'effectif de l'ASIO et de l'ASIS a doublé ou devrait doubler d'ici quelques années[58].

La préférence des organismes d'analyse pour des services de petite taille a été largement contestée pendant les périodes de controverse et les enquêtes. Les membres des comités parlementaires ont semblé vraiment estomaqués quand ils ont constaté que l'ONA comptait bien peu d'analystes pour

---

[56] *Ibid.*, pp. 12 et 13.

[57] *Ibid.*, p. 15.

[58] « Australia Doubles Spy Agency », SBS World News Headline Stories, 17 octobre 2005.

faire face à la somme croissante de renseignements qu'il reçoit sur des sujets comme l'Irak et le terrorisme. Le PJCAAD a ainsi appris qu'il comptait deux analystes experts du Moyen-Orient et qu'un seul spécialiste de l'analyse stratégique était chargé du dossier des ADM irakiennes et qu'ils « n'avaient pas travaillé exclusivement sur ce dossier pendant cette période » [59]. M. FLOOD a recommandé de doubler l'effectif de l'ONA en le faisant passer de 74 à 145 personnes et d'accroître son budget de 13,1 millions à 25 millions de dollars par an. Il a aussi conseillé de transférer le service responsable des sources ouvertes du MAEC à l'ONA, reconnaissant ainsi l'importance des informations tirées de ces sources et prenant acte du fait que les alliés de l'Australie leur accordent de plus en plus de poids. Cette recommandation contribuera à organiser la recherche et l'utilisation de ces informations et à les harmoniser avec les décisions prises en matière de collecte secrète de renseignements.

À la suite de cette augmentation soudaine de ses budgets et de ses effectifs, certains se sont demandés si l'AAR serait en mesure de recruter des personnes compétentes tout en maintenant ses normes et d'« accueillir » un nombre si élevé de nouveaux employés[60]. Les administrateurs des services de renseignement indiquent, en général, que contrairement à l'idée véhiculée par les médias, les demandes d'emploi pleuvent depuis le 11 septembre et depuis que le public s'intéresse davantage au renseignement. Les postes de niveaux plus subalternes, sauf ceux qui exigent des connaissances linguistiques et des compétences techniques particulières, ont pu être comblés sans aucune difficulté. L'AAR a adopté un processus de filtrage de sécurité et un cours de formation de base des jeunes recrues communs à tous les services. Dans le cas des postes de dirigeants ou ceux qui exigent des compétences bien précises, certains services ont constaté que le fait que leurs bureaux soient situés à Canberra, loin des grands centres urbains, les a empêchés d'attirer les personnes dont ils ont besoin. Certains ont dû faire face à une pénurie de cadres intermédiaires expérimentés et capables de diriger et d'encadrer de nouveaux employés et d'assurer le contrôle de la qualité. Dans les domaines où il y a une pénurie de candidats qualifiés, les services se sont livrés une certaine concurrence, mais ils ont résolu le problème ensemble. Les directeurs des services de l'AAR reconnaissent qu'une certaine mobilité entre les organismes favorise l'établissement de liens de communication et permet aux membres de l'AAR de mieux se comprendre les uns les autres.

4. Conclusion

Les récents changements au sein de l'AAR ont renforcé les principes structurants qui l'ont toujours guidé plus qu'ils ne les ont contestés. Les responsables des diverses commissions d'enquête et le gouvernement semblent avoir conclu que l'AAR devrait être en mesure de relever adéquatement les nouveaux défis et de corriger les erreurs passées s'il dispose des ressources nécessaires et si ces opérations sont bien coordonnées. Il est trop tôt pour dire si ces conclusions et les réformes qui en ont découlé lui permettront, en effet, de relever les défis associés aux menaces transnationales ou

---

[59] Rapport PJCAAD, p. 47.

[60] Voir, par exemple, Julie MACKEN, « I Spy a Problem on Intelligence », *Australian Financial Review*, 24 novembre 2005 et Deborah Snow, « A Shortage of Spooks », *Sydney Morning Herald*, 15 novembre 2004.

d'éviter les problèmes « familiers » et récurrents liés aux processus du renseignement ou, plus précisément, aux pressions politiques exercées sur les services de renseignement. Si ces défis s'avèrent trop importants pour être réglés par quelques changements structurels sans conséquence et l'ajout de ressources, il se pourrait que le prochain train de réformes importantes soit mis en place dans moins d'un quart de siècle.

Le professeur Michael WESLEY est directeur du Griffith Asia Institute à l'Université Griffith, en Australie. Avant d'occuper ce poste en juillet 2004, il était directeur général adjoint des dossiers transnationaux au Bureau des évaluations nationales. Avant de s'y joindre, il était maître de conférences à la School of Politics and International Relations de l'University of New South Wales, et chargé de recherches à l'Asia-Australia Institute, de la même université.